Windows To Go -ominaisuuden käyttöönotto ja hallinnointi

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Hämeen ammattikorkeakoulu, Tieto- ja viestintätekniikka

Riihimäki, kevät 2018

Joni Laakso

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

RIIHIMÄKI
Tieto- ja viestintätekniikka

Tekijä Joni Laakso **Vuosi** 2018

Työn nimi Windows To Go -ominaisuuden käyttöönotto ja hallinnointi

Työn ohjaajat Ilkka Koski, Teemu Järvenpää

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli Windows To Go -ominaisuuden esittely, käyttöönotto, hallinnointi lähiverkossa sekä etänä ja tietoturvallinen käyttö eri ympäristöissä. Opinnäytetyön toimeksiantajana toimi Puolustusvoimien tutkimuslaitos PVTUTKL. Toimeksiantaja toivoi lisäselvitystä työasemalle, joka on tietoturvallinen sekä liikkuva. Työaseman tulee olla helposti käyttöönotettavissa esimerkiksi ulkomaan komennuksilla, joissa henkilökohtaiset kannettavat eivät ole kustannustehokas ja mobiili ratkaisu. Työasemaa ei sijoiteta organisaation toimialueelle ja toimii näin tietoturvallisena internetkoneena.

Opinnäytetyössä käydään läpi projektin tavoitteet ja tehtävät, sekä käsitellään toiminnon kehityksen kannalta keskeisiä asioita. Esitellään Windows To Go -ominaisuus ja erot tyypillisen Windows-asennuksen kanssa, järjestelmävaatimukset sekä yritysominaisuudet. Toiminnallisessa osassa perehdytään Windows To Go USB-muistin käyttöönottoon eri menetelmillä. Opinnäytetyössä pilotoiduissa USB-muisteissa käyttöönottoon käytettiin ”Microsoft SCCM -hallinnointiohjelmaa”, ”Windows To Go Creator Wizard” sekä ”Windows PowerShell -komentotulkki ohjelmaa”. Työssä pohditaan eri ratkaisuja tietoturvalliseen etähallinnointiin ja asemien päivittämiseen ulkoisissa, sekä sisäisissä verkoissa. Lopuksi käydään läpi mahdollisia tietoturva ratkaisuja Windows To Go -ominaisuudelle ja näiden toteuttamista.

Lopputuloksena toteutettiin WTG -ominaisuuden käyttöönottopilotointi kolmella eri menetelmällä. Projektin tavoitteet saavutettiin ja asennusmediat olivat toimivia. Ominaisuuden kehitystyötä on mahdollista jatkaa annetuilla esimerkeillä ennen varsinaista käyttöönottoa.

Avainsanat Bitlocker to Go, käyttöönotto, PowerShell, SCCM, työasema, Windows To Go

Sivut 42 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Riihimäki
Information and Communication Technology

Author Joni Laakso **Year** 2018

Subject deployment and administration of Windows To Go feature

Supervisors Ilkka Koski, Teemu Järvenpää

ABSTRACT

The purpose of this thesis was to introduce the Windows to Go feature, its deployment and administration in the local network as well as remote access and secure use in different environments. The Finnish Defence Research Agency FDRA was the commissioner of this thesis. The commissioner wanted further research on a workstation that was to be both secure and mobile. The workstation needed to be easily deployed and used for example abroad, where personal laptops are not a cost effective or mobile solution. The workstation was not to be stationed in the organizations local area network but it was to work as a secure internet machine.

In this thesis, I go through the goals and tasks of the project, and cover the crucial points in the development of the feature. I go through the fundamentals with the Windows to Go feature as well as the differences there compared to a typical Windows workstation. I also cover system requirements to run Windows to Go and its enterprise features. In the empirical part I introduce Windows to Go USB flash drive deployment with multiple methods. In the thesis project the deployment of Windows to Go was piloted using “Microsoft SCCM configuration manager”, ”Windows to Go Creator Wizard” and “Windows PowerShell Command-line utility”. In this paper I go through different options for a secure remote access, such as VPN and DirectAccess. Lastly, I go through possible information security steps for Windows to Go and how to put these into practice.

As a result, the deployment of the WTG feature was piloted using three different methods. The objectives in the project were achieved, and the deployment medias were functional. The development of the feature can be prolonged with the given examples, before proper deployment.

Keywords Bitlocker To Go, deployment, PowerShell, SCCM, Windows to Go, workstation

Pages 42 pages

SISÄLLYS

1 JOHDANTO

Opinnäytetyön aihe-ehdotus tuli toimeksiantajalta, Puolustusvoimien Tutkimuslaitokselta PVTUTKL, jossa suoritin myös työharjoittelua. PVTUTKL on monitieteinen organisaatio, joka tuottaa vaativia puolustusalan tutkimus-, kehittämis- ja testauspalveluja useiden eri teknologioiden alueille. Toimeksiantaja toivoi lisäselvitystä työasemalle, joka on tietoturvallinen sekä liikkuva. Työaseman tulee olla helposti käyttöönotettavissa esimerkiksi ulkomaan komennuksilla, joissa henkilökohtaiset kannettavat eivät ole kustannustehokas ja mobiili ratkaisu. Työasemaa ei sijoiteta organisaation toimialueelle, ja työasema toimii näin tietoturvallisena internetkoneena.

Windows To Go on USB-asemalle asennettava versio käyttöjärjestelmästä. Asennus tukee Windows 8 ja Windows 10 Enterprise ja Education käyttöjärjestelmiä. Käyttöjärjestelmä toimii samalla tavalla, kuin tavallinen työpöytäasennus, muutamaa teknistä yksityiskohtaa lukuun ottamatta. Näitä eroavaisuuksia käsitellään myöhemmin työssä. Windows To Go on suunniteltu korvaavaksi vaihtoehdoksi kannettavalle tietokoneelle. Käyttäjälle voidaan antaa puhdas Windows -käyttöjärjestelmä versio tai vaihtoehtoisesti räätälöity asennus. Käyttäjä voi itse suorittaa asennuksen käyttäen ”Windows To Go Creator Wizard -ohjelmaa”. Asennusohjelma löytyy Enterprise ja Education -käyttöjärjestelmistä. Palvelinympäristössä asennuksen voi suorittaa ”Microsoft SCCM (System Center Configuration Manager) -hallinnointiohjelmalla”. Asennuksesta voidaan tehdä käyttäjille jaettava paketti tai hallinnointiohjelmassa suoritettava suora asennus. Ylläpitäjän oikeudet hallitseva käyttäjä voi suorittaa asennuksen myös PowerShell komentokehotteita (skriptejä) käyttäen.

Yksityisen sektorin käyttöön tullessa Windows To Go on ominaisuus, jolla etätyöntekijöille, alihankkijoille tai konsulteille voidaan antaa organisaation yksilöity työpöytä näkymä käyttöön tietoturvallisesti. Ominaisuudesta voi olla hyötyä esimerkiksi tilanteessa, jossa työntekijä tuo töihin oman laitteensa, joka on määritelty toiselle toimialueelle. Tällöin USB-asemalle asennettu käyttöjärjestelmä voidaan käynnistää työntekijän omalla koneella, silloisen osaston toimialueelle. Näin kaikki organisaation määrittämät asetukset ja tiedostot ovat käytössä, eikä organisaation tietoturva vaarannu missään vaiheessa.

Työ suoritettiin Hyper-V virtuaaliympäristöä käyttäen. Palvelimien versiot olivat Windows Server 2016. Testikäyttöjärjestelmänä toimi Windows 10 versio 1709 Enterprise Evaluation. Työ suoritettiin palvelimella käyttäen hallinnointiohjelmaa SCCM -versio 1702. Loput palvelimista toimi pääpalvelimen tukipalvelimina. Windows To Go USB-aseman luonti tapahtui pääpalvelimella ylläpitokäyttäjällä, käyttäen PowerShell -komentotilaa ja SCCM -hallinnointiohjelmaa. Pilotoitavana USB-asemana käytettiin Kingston DT workspace USB-muistia.

Opinnäytetyö on toiminnallinen perehdytys, jonka lopputuloksena on organisaation valmius käyttöönottaa ja kehittää mobiilia työasemaratkaisua erinäisissä ympäristöissä. Toiminnallisuus koostuu laitteen käyttöönoton suunnittelusta, ja mahdollisista etähallinnointiominaisuuksien implementoinneista. Työ koostuu pääosin Microsoftin julkaisuista, sekä omista havainnoista ja perehtymisestä aiheeseen, kuten ”Microsoft SCCM -hallinnointiohjelman” opiskelusta. Windows To Go -aseman pilotoinnin yhteydessä nousseet ongelmat auttoivat soveltamaan, ja hyödyntämään hankittuja tietoja ja taitoja.

2 WINDOWS TO GO

Windows To Go on suunniteltu niin, että käyttökokemus eroavaisuudet perinteisen työaseman ja USB-aseman välillä ovat minimoidut. Se eroaa kuitenkin tavallisesta Windows -käyttöjärjestelmästä muutamalla tavalla.

Isäntäkoneen sisäiset kovalevyt ovat offline-tilassa. Uudelleenkäynnistäessä WTG USB-asemalla isäntäkoneen sisäiset kovalevyt pysyvät oletuksena epäaktiivisina estäen tikun mahdollisen saastumisen tai isäntäkoneen tiedostoihin pääsyn. Mikäli WTG USB-asema kiinnitetään käynnissä olevaan koneeseen, asema ei ole havaittavissa Windows Explorer -näkymässä.

TPM (Trusted Platform Module) ei ole käytössä. TPM on kansainvälinen tietoturvastandardi, joka perustuu tietokoneen sisällä emolevyyn sijoitettuun fyysiseen mikrosiruun. TPM suojaa kiintolevyn tiedot mikrosiruun tallennetun salausavaimen avulla. Kiintolevyn suojaamisen lisäksi moduuli myös liittää käyttäjätunnuksen ja salasanan moduulin sisältävään tietokoneeseen eikä käyttöjärjestelmään. TPM on siis sidottu yhteen koneeseen ja WTG USB-asemat vaihtavat isäntäkonetta. TPM:n sijasta WTG USB-asema käyttää tietoturvaratkaisuna Bitlocker To Go -tekniikkaa. (Trusted Computing Group 2008.)

Hibernation eli lepotila on poissa käytöstä oletuksena. Lepotilan ollessa päältä pois voidaan USB-asemaa liikuttaa helpommin koneesta koneeseen ja vältetään tahaton irrotus USB-aseman ollessa päällä ja tästä johtuvat mahdolliset tiedoston menetykset. Lepotilan saa kuitenkin päälle halutessaan Group Policy -säännöllä. (Microsoft 2017.)

Windows Recovery Environment eli järjestelmän palautus ei ole mahdollista. Mikäli WTG USB-asema tarvitsee järjestelmän palautuksen, tulee se formatoida ja uudelleenasentaa näköistiedosto. Mikäli USB-asema siis lakkaa käynnistymästä, ovat tiedostot siis palautumattomat. (Ballew 2016, 5.)

Windows To Go USB-aseman käyttöjärjestelmää ei ole mahdollista päivittää. Vanhempia Windows 8, WTG USB-asemia ei ole mahdollista päivittää Windows 10 -versioon, eikä Windows 10 -versiosta ylöspäin. Mikäli työasemalle halutaan uusi versio, tulee USB-asema asentaa uudelleen päivitetyllä näköistiedostolla. (Ballew 2016, 68.)

Windows To Go tukee myös laitteiston tunnistusta. Kun WTG-asema käynnistetään ensimmäistä kertaa esimerkiksi kotona sijaitsevalla tietokoneella, tunnistaa asema tietokoneen laitteiston ja asentaa tarvittavat ajurit. Seuraavan kerran käynnistäessä sama WTG USB-asema samalla isäntäkoneella tunnistaa asema laitteiston tunnetuksi, nopeuttaen huomattavasti käynnistystä. (Ballew 2016, 121.)

Kaikki fyysinen laitteisto isäntäkoneessa, kuten USB-portit, verkkokortti, näytön liittimet tai kuulokeliitännät ovat tunnistettuja ja toiminnallisia Windows To Go -ympäristössä. Vain isäntäkoneen kovalevyt ovat poissa käytöstä, jotta käytettävän koneen tiedostot eivät vaarannu.

2.1 **Laitevaatimukset**

On hyvin suositeltavaa, että Windows To Go -asemat asennetaan vain sertifioiduille USB-asemille, jotka ovat erityisesti valmistettu Windows -käyttöjärjestelmän käynnistämistä ja käyttöä varten. Jotta USB-asema saa sertifikaatin, tulee USB-muistin läpäistä Microsoftin sertifiointitestit, ja läpikäydä suorituskykytestit eri työasema kokoonpanoilla. Näin valmistaja takaa hyvän suorituskyvyn isäntäkoneesta tai käyttöjärjestelmästä riippumatta. Kyseiset WTG -sertifioidut USB-asemat ovat rakennettu nopeita luku- ja kirjoitus nopeuksia varten hyvällä random access I/O suorituskyvyllä eli satunnaistiedostonlukunopeudella. Sertifioiduissa USB-asemissa on myös pidemmät valmistajan takuut, sekä automaattisesti asentuvat ajurit useimmille malleille. (Microsoft 2013.)

Koska Windows To Go käyttää isäntäkoneen komponentteja toimiakseen on tärkeää, että USB-asema ja käytössä oleva työasema ovat yhteensopivat. WTG USB-asema toimii isäntäkoneissa, joissa on Windows 7 tai uudempi käyttöjärjestelmä. Poikkeuksena Windows RT, joka on Windows 8 käyttöjärjestelmän 32-bittinen versio pääosin kosketusnäytöille. Windows To Go -työasemat eivät myöskään tue MacOS-käyttöjärjestelmää. Itse WTG-asennus vaatii Enterprise tai Education -käyttöjärjestelmä version.

Windows To Go -asema on tarkoitettu käytettäväksi USB3.0 portissa, mutta tuki löytyy myös USB2.0 portille. Isäntäkoneessa on oltava USB-käynnistysmahdollisuus. WTG-aseman käynnistys konfigurointitapoja on kaksi. Windows 8 ja 10 käyttöjärjestelmissä, joko työpöytä näkymässä kirjoittamalla Windows hakuun ”Change Windows To Go startup options” ja klikkaamalla täplän hyväksyvään vaihtoehtoon. Mikäli kyseistä asetusta ei isäntäkoneelta löydy tulee se tehdä laitteen BIOS-asetuksista, vaihtamalla

ensisijaiseksi käynnistys järjestykseksi USB-asemat. Windows 7 käyttöjärjestelmässä, joudut muuttamaan BIOS -asetuksiasi USB-käynnistystä varten, sillä kyseisessä käyttöjärjestelmässä ei ole virallista Bitlocker To Go käynnistys tukea. BIOS-asetuksiin pääset painamalla koneen käynnistyessä funktio näppäintä F1, F2 tai F12 riippuen valmistajasta. BIOS -asetuksissa ollessasi, tarkista että USB-käynnistystuki on päällä, ja tämän jälkeen muuta ensisijaiseksi käynnistys järjestykseksi USB-asemat ennen muita. USB-käynnistys tuen lisäksi on WTG-asemalle asennettava isäntäkoneen prosessori arkkitehtuurin ja laiteohjelmiston kanssa yhteensopiva WTG -käyttöjärjestelmä asennusmedia. Kuvasta (Kuva 1) löydämme yhteensopivat käyttöjärjestelmän versiot. (Microsoft 2017.)

Host PC Firmware Type	Host PC Processor Architecture	Compatible Windows To Go Image Architecture
Legacy BIOS	32-bit	32-bit only
Legacy BIOS	64-bit	32-bit and 64-bit
UEFI BIOS	32-bit	32-bit only
UEFI BIOS	64-bit	64-bit only

Kuva 1. Arkkitehtuurillinen yhteensopivuus isäntäkoneen ja Windows To Go -aseman välillä (Microsoft 2017.)

2.2 **Käyttösuositukset**

Windows To Go on kaiken kaikkiaan hyvin yksinkertainen käyttää. Käyttäjien tulisi kuitenkin noudattaa muutamaa ohjesääntöä, saadakseen kaiken irti USB-asemasta ja varmistaakseen ominaisuuden toimivuuden.

- Sammuta Windows aina käytön jälkeen, ja odota sammumisen loppuun asti ennen Windows To Go -aseman poistoa.
- Vältä kiinnittämästä Windows To Go -asemaa jo käynnissä olevaan tietokoneeseen.
- Windows To Go -aseman käynnistys USB-telakan kautta ei ole tuettu. Kiinnitä asema aina porttiin, joka on suoraan yhteydessä emolevyyn.
- Mikäli koneesta löytyy USB3.0 portti, liitä asema ensisijaisesti tähän, Windows To Go on kuitenkin myös yhteensopiva USB2.0 portin kanssa.
- Windows To Go -asema tukee vain Microsoftin omia virallisia USB-ajureita.
- Mikäli Isäntäkoneesta löytyy tiedoston salausohjelma kuten Bitlocker, tulee se ensin kytkeä päältä pois, ennen kuin BIOS muutokset tehdään USB-käynnistystä varten.

(Microsoft 2017.)

2.3 **Yritysominaisuudet**

Varustettaessa yritystä tai organisaatiota Windows To Go:ta varten tulee ottaa huomioon muutama seikka. WTG toimii vain Enterprise tai Education käyttöjärjestelmäversioilla, joten se vaatii yritykseltä volyymikäyttöoikeussopimuksen Microsoftin kanssa. Tavallisesti organisaation työntekijöille tarjotaan työasema, jonka käyttöjärjestelmä ja ohjelmat on aktivoitu volyymikäyttöoikeusavaimella MAK (Multiple Activation Key) tai KMS (Key Management Service). MAK-avaimilla voidaan aktivoida yksittäisiä tietokoneita tai tietokoneiden ryhmiä muodostamalla suora yhteys Microsoftin palvelimiin. Lisenssiavainten käyttökertojen määrä on rajoitettu organisaation ja Microsoftin välisellä volyymikäyttöoikeuslisenssillä. KMS on organisaation sisäisesti ylläpitämä palvelu, jonka avulla Windows -pohjaiset tietokoneet ja ohjelmat voidaan aktivoida automaattisesti. KMS-palvelun käyttöön vaaditaan vähintään 25 verkossa olevaa tietokonetta. KMS-palvelun kautta aktivoidut tietokoneet ja ohjelmat on aktivoitava uudelleen muodostamalla yhteys organisaation verkkoon KMS-palvelimen ylläpitäjien määrittämän ajan välein, esimerkiksi kuukauden välein. Mikäli KMS-palvelimeen ei saada yhteyttä määritetyn ajan kuluessa, ohjelmien ja käyttöjärjestelmän lisenssit muuttuvat mitätöidyiksi.
(Microsoft 2018.)

Organisaation työntekijöiden käyttäessä Microsoftin lisenssiä vaativia ohjelmia kuten Officea on Windows To Go -asemalle suositeltavaa syöttää KMS -volyyymikäyttöoikeusavain. Mikäli Microsoft Office on asennettu käyttäen MAK-avainta, ohjelma vaatii uuden käyttöoikeusavaimen aina, kun WTG käynnistetään uudessa koneessa. MAK-avain tarkistaa koneen voimassa olevan lisenssin työaseman laitteiston kanssa. Tarkoittaen täten, että mikäli koneen prosessori tai emolevy vaihdetaan, mitätöityy lisenssiavain. Kun kyseessä on WTG, jota tullaan useimmiten käyttämään monessa eri työasemassa, vaatii Office uudelleen aktivointia. Vaikka organisaation kaikki työasemat olisivat identtisiä keskenään, vaatii WTG uudet aktivoinnit sillä, laitteistolla on eri ID-avaimet. KMS-avainta käytettäessä kyseistä ongelmaa ei synny palvelin autentikoinnin ansiosta ja ohjelma pysyy aktivoituna. Microsoft Office -versioista organisaation tulisi käyttää Proplus tai Enterprise versiota.

3 WINDOWS TO GO KÄYTTÖÖNOTTO

Windows To Go USB-asema voidaan luoda kolmella eri tavalla:

- "Windows to Go Creator Wizard" Windows 8 ja 10 Enterprise ja Education versioissa
- PowerShell
- System Center Configuration manager 2012 ja 2016

Asemalle voidaan antaa asennus näköistiedostoksi tyhjä Windows-käyttöjärjestelmä tai organisaation muokkaama Windows-käyttöjärjestelmä, josta löytyy valmiiksi tarvittavat ohjelmat, lisenssit sekä toimialueet. Yksinkertaisin USB-aseman luonti tapahtuu käyttämällä, "Windows To Go Creator Wizardia". Tästä luontitavasta puuttuu muun muassa moniajoasennus sekä yksityiskohtaisemmat muokkaus mahdollisuudet.

PowerShell -komentotulkki ohjelmalla asennus luodaan manuaalisesti käyttäen komentosarjoja. PowerShell -komentosarjoilla voidaan USB-asema luoda automatisoidusti tukien moniajoasennusta merkittävillä muokkausmahdollisuuksilla.

USB-aseman luonti "Microsoft SCCM:llä (System Center Configuration Manager)" on kaksivaiheinen, jossa ensin määritellään Windows To Go -näköistiedosto ja mitä ohjelmia tai asetuksia käyttöjärjestelmälle määritellään. Toiseksi määritellään itse USB-aseman asetukset, kuten Bitlocker To Go tai asematunnuksen määrittely. Kyseiset vaiheet toteuttamalla voidaan asennuksesta tehdä IT-hallinnolle äärimmäisen helppo ja nopea ratkaisu. SCCM toteutuksella voidaan hallita suuria määriä asemia ja pitää niillä hyvä käytettävyystaso mahdollisimman pienellä ylläpidolla.

3.1 Microsoft SCCM

System Center Configuration Manager eli SCCM on Microsoftin kehittämä keskitetty järjestelmänhallintaohjelma Windows -käyttöjärjestelmille. Sovelluksella järjestelmänvalvojat voivat hallita organisaation Windows-pohjaisten järjestelmien ylläpitoa koko laitteen elinkaaren ajan. Sovelluksen avulla organisaation on helpompaa hallita päivitysten jakelua sekä ylläpidettävyyttä. Tämä sisältää työasemien käyttöönoton ja hallinnoinnin sekä ohjelmien jakamisen. System Center Configuration Manager mahdollistaa keskitetyn ja joustavan laitteistojen hallinnan, ohjelmistopakettien asentamisen, sekä tietoturvaratkaisun.
(University of Nebraska-Lincoln 2018.)

Ennen kuin Windows To Go -asennusmedian luonti voidaan aloittaa sovelluksella, on suoritettava kolme vaihetta. Windows PE -käynnistysnäköistiedosto tulee löytyä jakelupisteeltä. Käynnistysnäköistiedostoa käytetään

asentamaan käyttöjärjestelmä kohde asemalle. Windows PE käynnistää käyttöjärjestelmän asennuksen, sekä asentaa asennukselle tärkeät laite ajurit. Toisessa vaiheessa Windows -käyttöjärjestelmä näköistiedosto tulee löytyä jakelupisteeltä. Käyttöjärjestelmä näköistiedostot ovat .WIM formaatissa olevia kompressoituja käyttöjärjestelmä asennuspaketteja. Viimeisessä esiasennusvaiheessa luodaan tehtävä jono eli Task Sequence. Task Sequence on paketti, joka määrittelee asennuksen aikana suoritettavat komennot. Task Sequence suorittaa määritellyt toimenpiteet, kuten formatointi ja partitiointi sekä käyttöjärjestelmän asennus jne. Toimenpiteet tapahtuvat järjestyksessä, jossa ne on asetettu Task Sequenceen. Task Sequence toimii WTG-käyttöjärjestelmä asennuksen runkona. Oletetaan esiasennusvaiheet valmiiksi suoritetuiksi SCCM -ympäristössä. (Microsoft 2016.)

On myös otettava huomioon SCCM -asennuspakettien käyttöönotossa asennuskoneen yhteys hallinnointipalvelimen toimialueelle. Asennettavat ohjelmat ja työkalut noudetaan asennuksen aikaan jakelupisteeltä. Mikäli asennettava työasema ei ole asennuksen aikana toimialueella, ei asennuksen aikana voida noutaa tarvittavia tiedostoja.

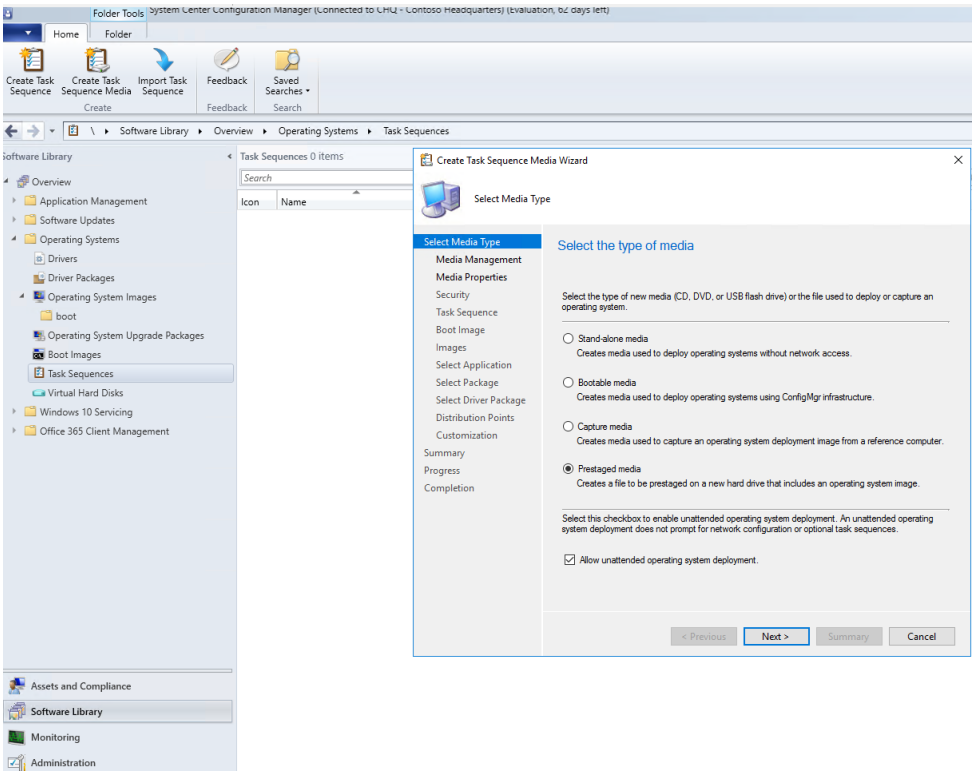
Koneen uudelleen käynnistäessä asennuksen jälkeen, WTG-asema käynnistyy Windows PE -tilassa. Asema yhdistyy hallinnointipisteeseen, josta asennuspaketissa määritetyt säännöt haetaan. SCCM hallinnointi sovellus määrittelee ja alustaa aseman. Alustuksen jälkeen asema voidaan käynnistää uudelleen viimeistelläkseen varustus prosessin, kuten ohjelmien ja työkalujen asennuksen. (Microsoft 2016.)

3.1.1 Prestaged Media

Prestaged Media sisältää käynnistysnäköistiedoston, sekä käyttöjärjestelmän näköistiedoston, joka asennetaan määrätylle asemalle. Asema, joka varustetaan Prestaged Media paketilla, käynnistetään käynnistysnäköistiedostolla. Tämän jälkeen asema voi aloittaa käyttöjärjestelmän käyttöönoton aiemmin luodusta Task Sequencesta, joka on määritelty pakettiin mukaan. Mikäli Task Sequence on puhdas käyttöjärjestelmä, voidaan Prestaged Media pakettiin lisätä tarvittavat sisällöt, kuten ohjelmat ja ajurit. Tämä vähentää käyttöjärjestelmän asennusaikaa ja verkon liikennettä, sillä ne löytyvät tällöin jo valmiiksi asemalta.

Aloita Prestaged Media paketin luominen avaamalla Configuration Manager -konsoli ja paina ”Software Library”. Ohjelmakirjasto työtilassa laajenna Operating Systems -kansio, ja tämän jälkeen paina ”Task Sequences”. Sovelluksen käyttöliittymän yläpalkissa löytyy painike ”Create Task Sequence Media”, jolla paketin luonti aloitetaan. Paketin luonti ohjelman avautuessa valitaan ensin paketille asennusmedian tyyppi. Valitaan ”Prestaged Media”, joka luo käyttöjärjestelmän sisältävän asennustiedos-

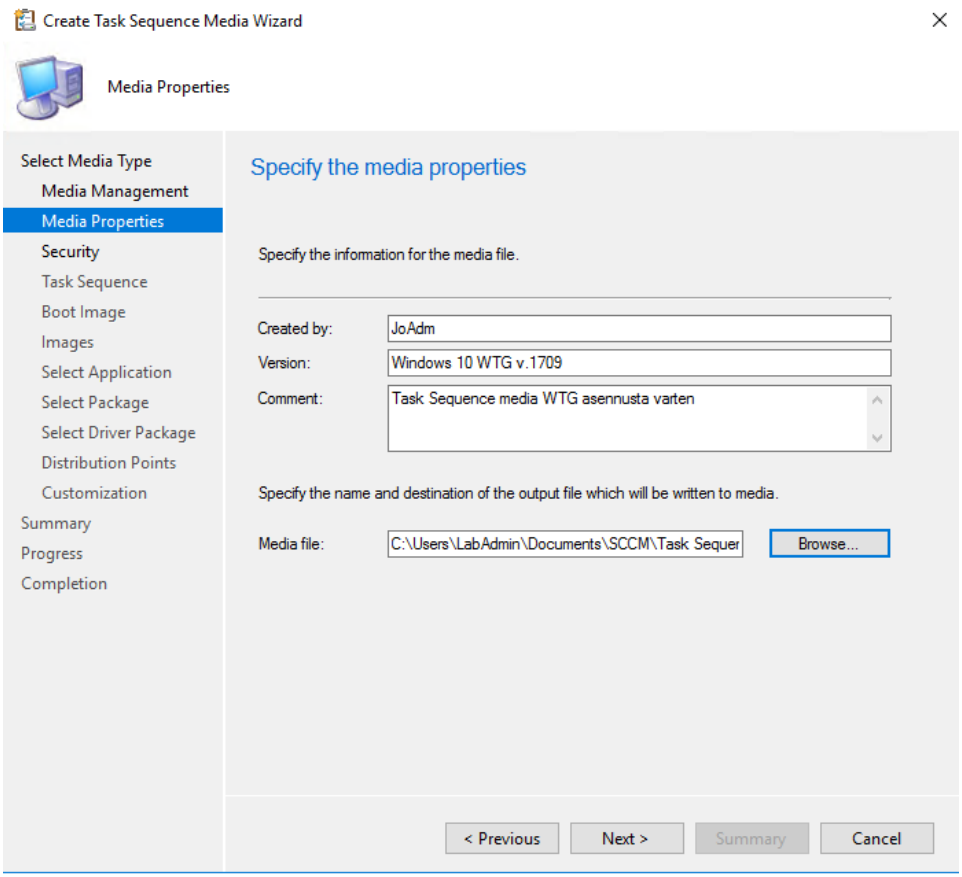
ton uudelle asemalle. Merkataan myös aktiviiseksi valintaruutu, jossa määritellään paketin asennuksen tapahtuvan automaattisesti ja ilman käyttäjän toimia. Myöhemmin paketin luonnissa määritellään muuttuja SMSTSPreferredAdvertID, jolla WTG käynnistyy automaattisesti ensisijaisena asemana isäntäkoneeseen kytkettäessä. Mikäli paketin asennus automatisointi asetus on hyväksytty ilman muuttujan lisäystä, esiintyy virhe asennusta suorittaessa. Kuvassa (Kuva 2) nähdään sijainti, jossa paketin luonti aloitetaan sekä Prestaged Media -paketin valinta. (Microsoft 2016.)



Kuva 2. Prestaged Media- paketin luonnin aloittaminen

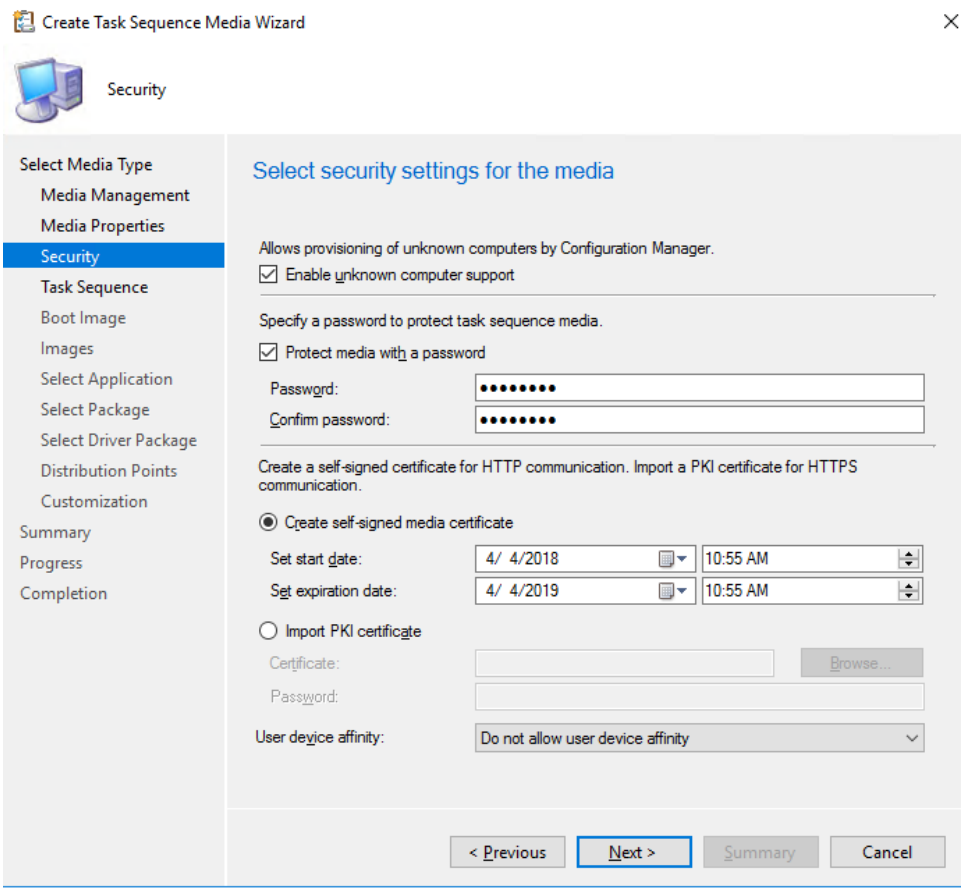
Media Management -sivulla määritellään, käytetäänkö asennuksessa medioita, kuten ohjelmia, ajureita tai skriptejä useammalta kuin yhdeltä palvelimelta. Mikäli organisaation SCCM media kansiot ovat hajautuneet useammalla palvelimelle valitaan Dynamic media -vaihtoehto. Dynamic media antaa luvan uudelleenohjata media tiedostoja hallinta pisteeltä toiselle. Tiedostojen ollessa kaikki samalla palvelimella valitaan Site-based media valinta. Site-based media ottaa yhteyden vain määrättyyn hallinta pisteeseen.

Media Properties -sivulla määritellään asennusta spesifioivat tiedot. Kuvassa (Kuva 3) nähdään kyseisessä asennuksessa määritellyt tiedot, sekä paketin tuloste sijainti.



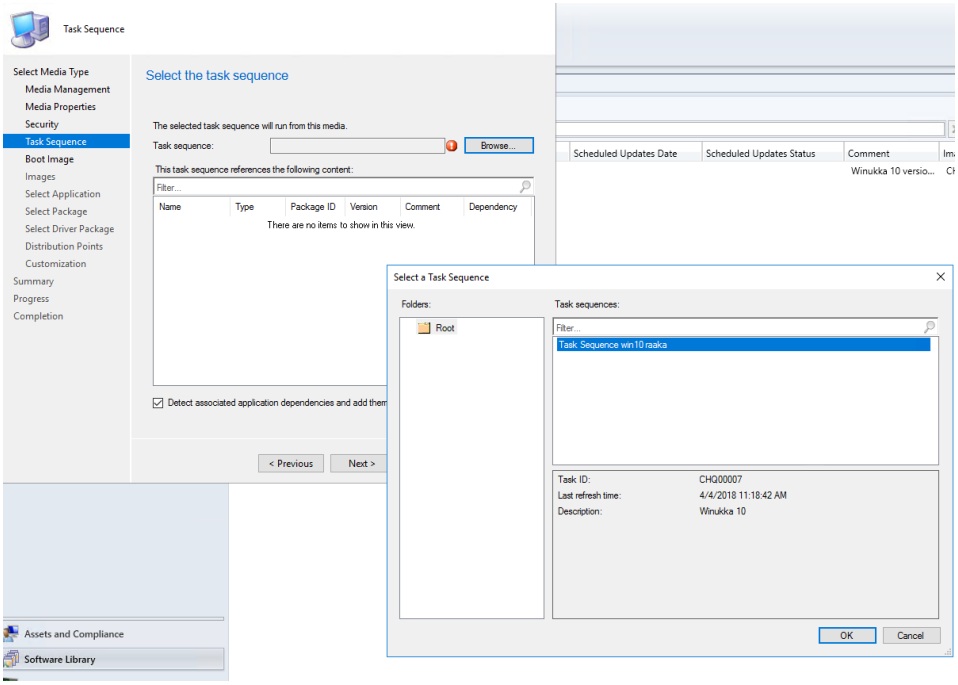
Kuva 3. Asennuspaketin tietojen täsmentäminen

Security sivulla -määritellään Prestaged Media -paketin turvatoimet. Valintaruudussa ”Enable unknown computer support” sallitaan median asennus tuntemattomalle asemalle, eli tietokoneelle joka ei ole SCCM ohjelman hallinnointi piirissä. Asennus mitä todennäköisimmin tapahtuu tunnetulla koneella, mutta varmuuden vuoksi ruutu merkitään aktiiviseksi. Tietoturvasyistä määritellään asennusmedialle salasana. Salasana suojaa paketin käyttöönottoa luvattomasti. Salasanan määritettyä käyttäjältä kysytään automatisoidussa asennuksessakin salasanaa ennen asennuksen aloittamista. Seuraavaksi määritellään yhteysmuoto, jolla aseman tiedostoja vastaanotetaan ja siirretään verkossa. Windows To Go -aseman tullessa verkkokäyttöön valitaan HTTP-yhteys -vaihtoehto, jolloin luodaan self-signed media sertifikaatti. Määritetään sertifikaatin kesto, joka tässä tapauksessa kestää vuoden, jolloin asema tulee asentaa uudelleen tai sertifikaatti uusia. ”User device affinity” -valinnassa määritellään, liitetäänkö käyttäjätili, tietokonetiliin. Mikäli asema annetaan vain yhden henkilön käyttöön, voidaan tilit yhdistää automatisoidusti tai ylläpitäjän toimesta, jolloin laitteen seuranta ja käyttäjä seuranta helpottuu. Tässä tapauksessa valitaan vaihtoehto, jossa tätä yhteyttä ei muodosteta, sillä laite poistuu hallintaverkosta ja tällä voi olla useampi käyttäjä. Kuvassa (Kuva 4) esimerkki määritykset asennus medialle.



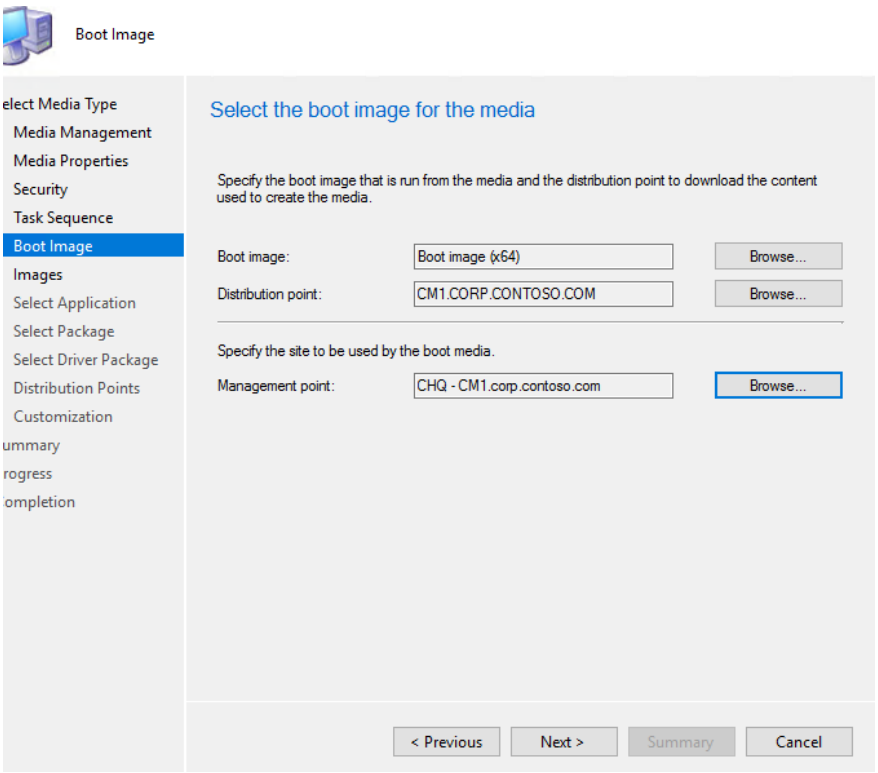
Kuva 4. Turvaus asetusten määrittely

Task Sequence -sivulla määritetään Windows -käyttöjärjestelmä asennus-paketti, joka on luotu esiasennusvaiheessa. Kuvassa (Kuva 5) luotu Task Sequence Windows 10 käyttöjärjestelmästä, joka asennetaan Windows To Go -asemalle.



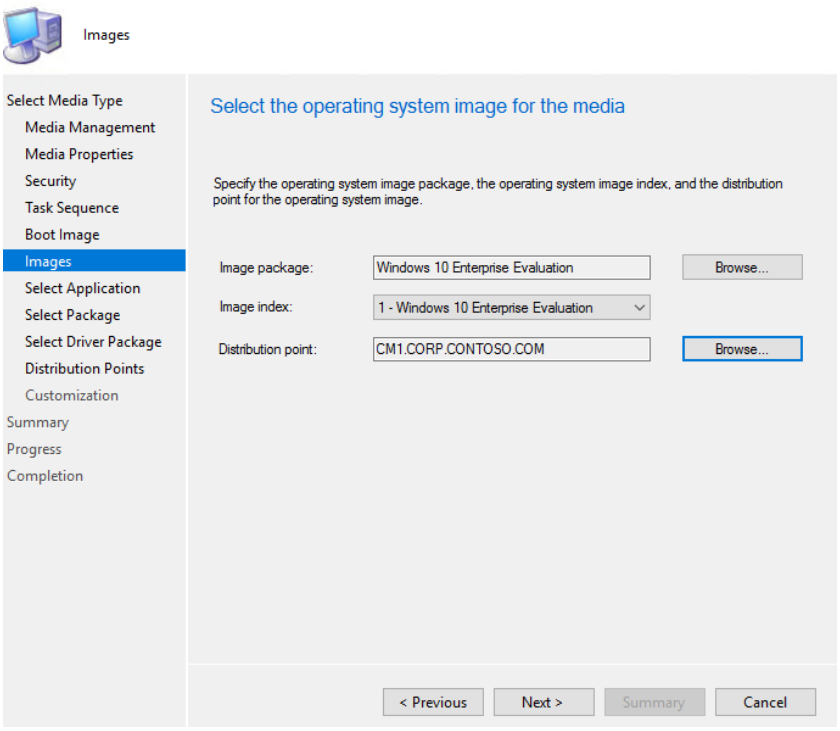
Kuva 5. Task Sequencen valinta asennusmediaan

Boot Image -sivulla määritetään käynnistysnäköistiedosto, jolla asema käynnistetään eli Win PE. Valitaan käyttöjärjestelmän kanssa yhteensopiva käynnistysnäköistiedosto eli tässä tapauksessa x64 (64-bittinen). Etsitään jakelupiste, jossa käynnistysnäköistiedosto sijaitsee. Asennusohjelma etsii käynnistysmedian tältä jakelupisteeltä ja kopioi sen asennuspakettiin. Määritetään vielä hallintapiste käynnistysmedialle. Kuvassa (Kuva 6) käynnistysnäköistiedosto, sekä virtuaaliympäristön jakelu- ja hallintapiste.



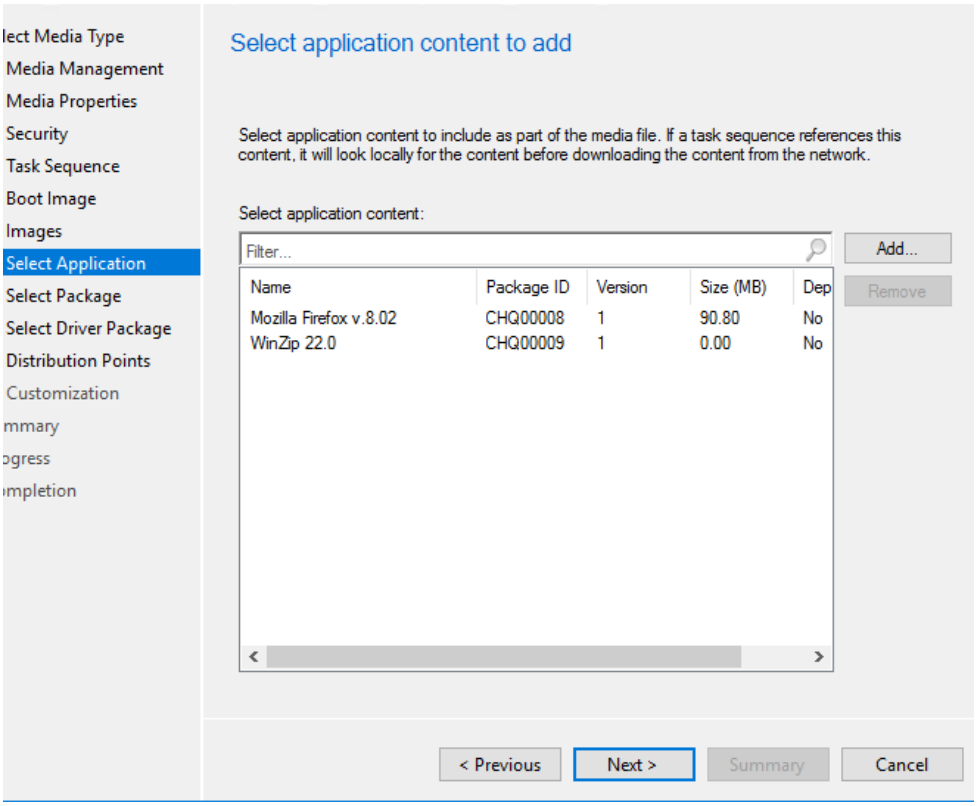
Kuva 6. Win PE käynnistysnäköistiedoston, sekä asennusmedian jakelu- ja hallinnointipisteen määrittely

Images -sivulla määritetään käyttöjärjestelmä näköistiedosto, sekä käyttöjärjestelmän versio ja jakelupiste, josta näköistiedosto noudetaan. Kuvassa (Kuva 7) Windows 10 Enterprise Evaluation näköistiedosto ja virtuaaliympäristön mediapalvelin.



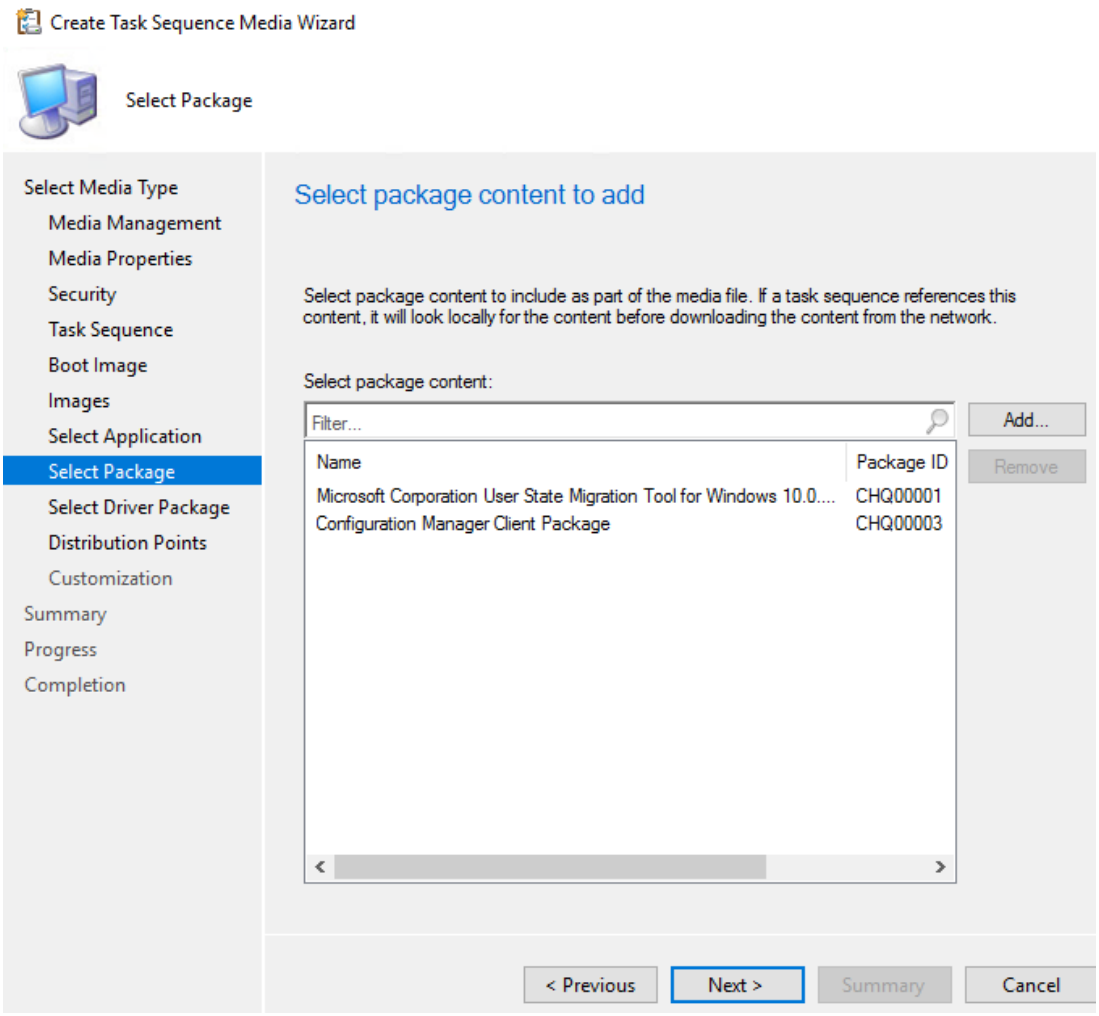
Kuva 7. Käyttöjärjestelmän lisääminen ja median jakelupisteen määrittely

Select application -sivulla määritellään Prestaged Media pakettiin lisättävät ohjelmat. Ohjelmat on lisätty esiasennusvaiheessa SCCM media palvelimelle, ja mainostettu jakelupisteille. Ohjelmien tulee olla .msi tiedostomuodossa, jotta asennus onnistuu ilman käyttäjän toimia. Valitsemme kaksi palvelimelle lisättyä ohjelmaa, Mozilla Firefox ja Winzip. Kuvasta (Kuva 8) nähdään valitut asennettavat ohjelmat ja painikkeen ”add”, jonka kautta ohjelmat haetaan jakelupisteeltä.



Kuva 8. Valitse asennettavat ohjelmat Windows To Go -asemalle

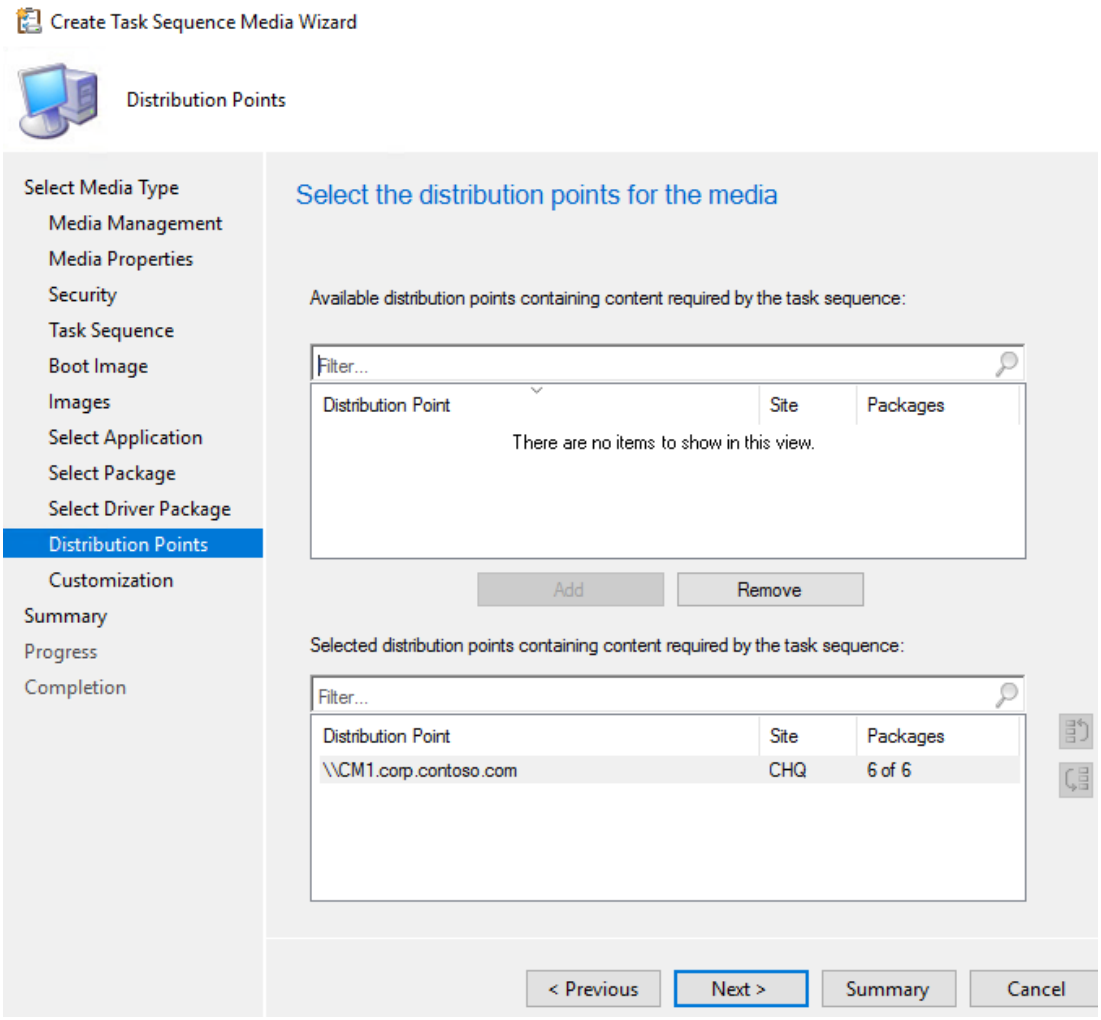
Select Package -sivulla valitaan asennuspaketteja, joita asennukseen halutaan sisällyttää. Paketteihin kuuluu esimerkiksi SCCM Client Package eli käyttäjälle asentuva SCCM portaali kuten Software Center. Asennuspaketti tulee lisätä Prestaged Media pakettiin, mikäli se on referoituna Task Sequencessa. Paketti etsii ensisijaisesti tietoa paikallisesti, ennen kuin se hakee paketin verkon yli. Kuvassa (Kuva 9) näemme kaksi mahdollista vaihtoehtoa lisättäväksi pakettiin. Aseman kuitenkin tullessa verkkokäyttöön ei kumpaakaan työkalua lisätä esimerkkiasennukseen.



Kuva 9. Asennusmediaan lisättävät työkalut

Select Driver Package -sivulla, Prestaged Media pakettiin voidaan lisätä laiteajurit, esimerkiksi organisaatiossa käytettävän kannettavan tietokoneen mallin mukaan. Windows To Go -sertifioiduissa USB-asemissa kuitenkin on valmiiksi asennettuna useimpien laitevalmistajien laiteajurit, joten tämän vaiheen voi ohittaa.

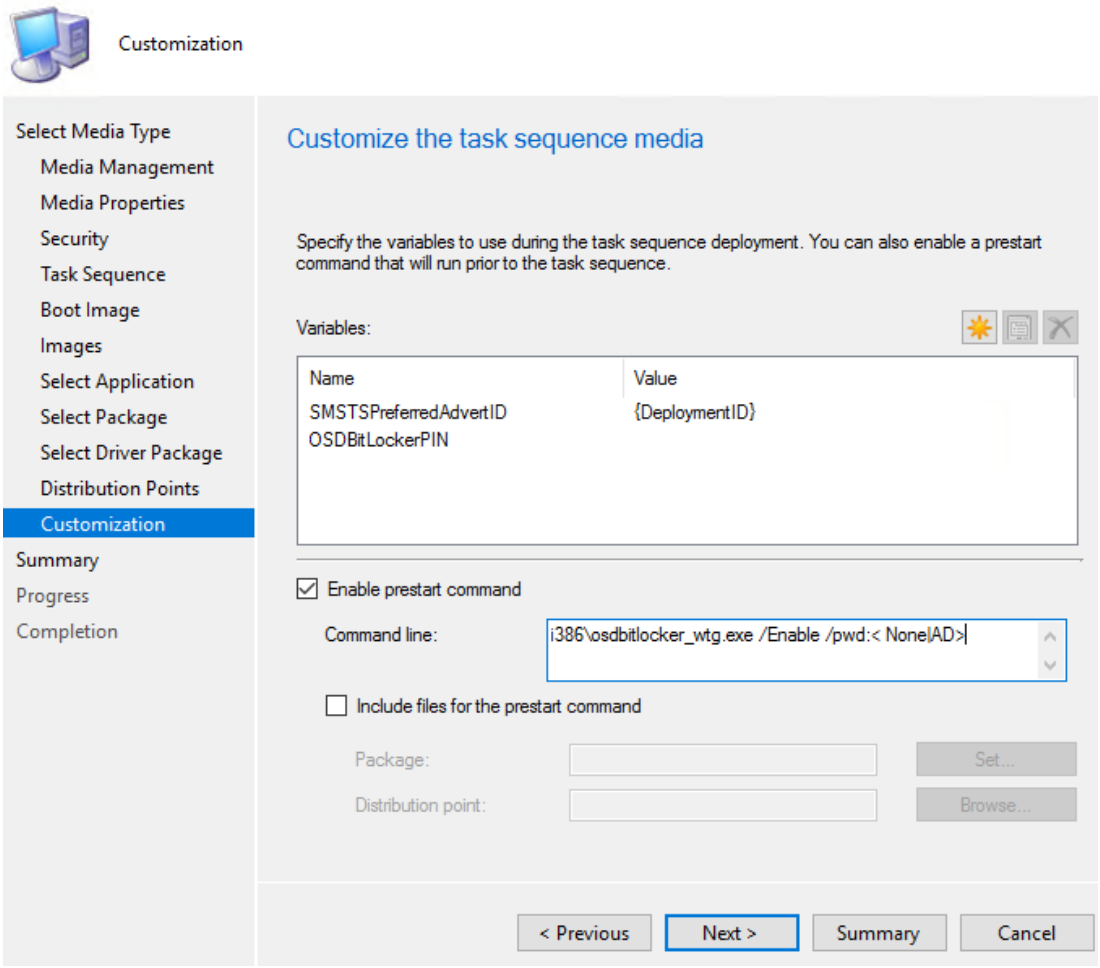
Distribution Points -sivulla valitaan jakelupisteet, joista asennuspaketin tiedostot tulevat. Kuvassa (Kuva 10) nähdään, kuinka kaikki kuusi asennuspakettiin kuuluvaa tiedostoa sijaitsee samalla jakelupisteellä, joten yhden jakelupisteen lisäys riittää. Mikäli mediatiedostot olisivat hajautettuina eri jakelupisteille tulisi nämä kaikki lisätä, jotta asennus osaisi viitata oikeaan verkkosijaintiin.



Kuva 10. Jakelupisteen määrittely, josta asennuspaketti hakee asennettavat ohjelmat

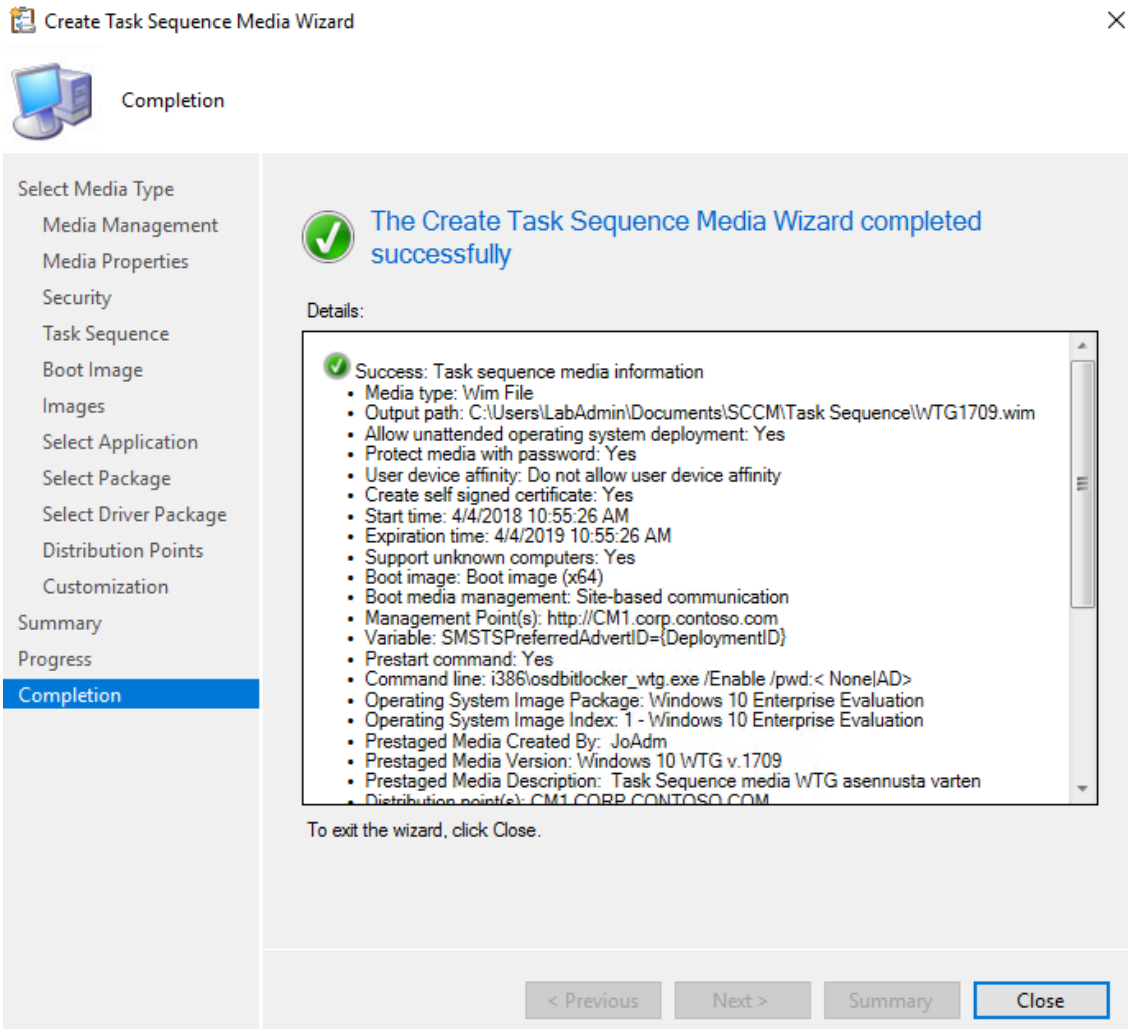
Customization -sivulla lisäämme paketin asennukseen mahdolliset muuttujat. Muuttuja luodaan painamalla kuvassa (Kuva 11) näkyvää keltaista tähteä. Määritellään muuttuja ”variable” ja annetaan tälle arvo ”value”. Asennukseen lisätään alussa mainittu SMSTPreferredAdvertID muuttuja. Isäntäkone käynnistää automaattisesti Windows To Go:n, kun se tunnistaa WTG USB-aseman. Määritellään muuttujan arvoksi vielä {DeploymentID}, joka luo ID tunnuksen liitettäväksi Task Sequencen kanssa, jolla WTG asennus suoritetaan. Lisäksi luodaan OSDBitlockerPin muuttuja, sekä komentorivillä näkyvä komentokehoite, jolla aktivoidaan Bitlocker To Go, WTG USB-asemalle. (Microsoft 2016.)

Tiedostonsalaus komentokehoite jätetään vielä tässä vaiheessa asennusta lisäämättä. OSDBitlockerPin tulee kuitenkin sisällyttää muuttujana, mahdollista tiedostonsalausta varten. Tiedostonsalauksen lisäys tehdään asennuspakettiin Bitlocker To Go -asennustyökalun teon jälkeen, joka tapahtuu seuraavassa aiheessa.



Kuva 11. Asennukseen lisättävien muuttujien määrittely

Summary -sivulla nähdään yhteenveto Prestaged Media pakettiin tulevista säännöistä. Painetaan ”Next” painiketta ja aloitetaan paketin luonti. Paketin rakentuessa nähdään edistymispalkki, ja se kestää 20-30 minuuttia. Paketin luonnin valmistuessa nähdään vielä kertaalleen yhteenveto sisällöstä, kuvassa (Kuva 12) esimerkki työn yhteenveto. Prestaged Media pakettia voi vielä jälkeenpäin muokata ”Task Sequences” valikossa ja klikkaamalla hiiren oikealla painikkeella mediaa, sekä valitsemalla täältä ”edit”. Asennuksessa luotua .WIM tiedostoa voidaan käyttää ylläpidon toimesta WTG USB-aseman luonnissa. Sisälletyt säännöt ja ohjelmat ovat sijoitettuna kyseiseen tiedostoon ja asentuvat asemalle automaattisesti ilman käyttäjän toimia.



Kuva 12. Prestaged Media paketin luonnin yhteenveto

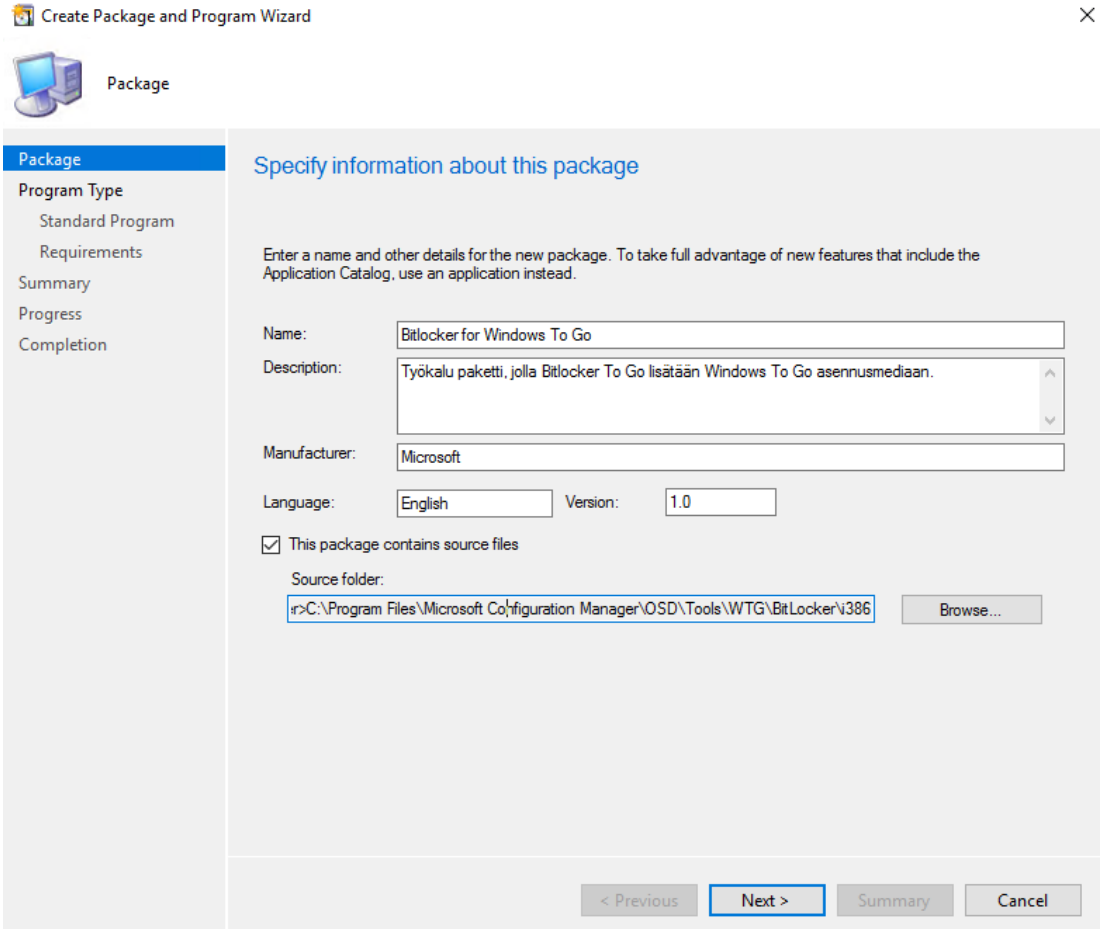
Windows To Go -asennuspaketti on myös mahdollista jakaa käyttäjille omatoimista asennusta varten. Käyttäjä lataa luodun .WIM asennuspaketti tiedoston omalle työasemalle ”Software Center” tiedostonjako ohjelmasta. Asennuspaketin latauksen jälkeen käyttäjän tarvitsee vain avata ”Windows To Go Creator” asennustyökaluohjelma ja valita asennusmediaksi ladattu paketti. Kyseisellä menetelmällä voidaan vähentää huomattavasti ylläpidon roolia työaseman asennuksessa.

3.1.2 Bitlocker To Go sisällytys SCCM asennusmediaan

Windows To Go mahdollistaa tiedostonsalauksen käytön ulkoisella asemalla, ilman TPM moduulia. Tiedoston salauksen lisääminen ulkoiselle asemalle SCCM:llä tapahtuu erillisellä työkalulla osdbitlocker_wtg.exe. Käyttöönotettaessa tiedostonsalaus, tulee Prestaged Media pakettiin lisätä komentokehoite, sekä luoda sovelluspaketti, johon tiedostonsalaus työkalu määritellään. (Microsoft 2016.)

Komentokehoite luotiin ”Prestaged Media” muuttujat -sivulla (kts. Prestaged Media ”Customization”). Kutsujan ollessa määritelty, voidaan aloittaa työkalun määritys. Aloita valitsemalla ”Software Library” SCCM Configuration Manager sovelluksessa ja laajenna näkymä ”Application Management”. Valitse ”Packages” näkymä ja paina vasemmassa yläkulmassa sijaitsevaa ”Create Package” painiketta.

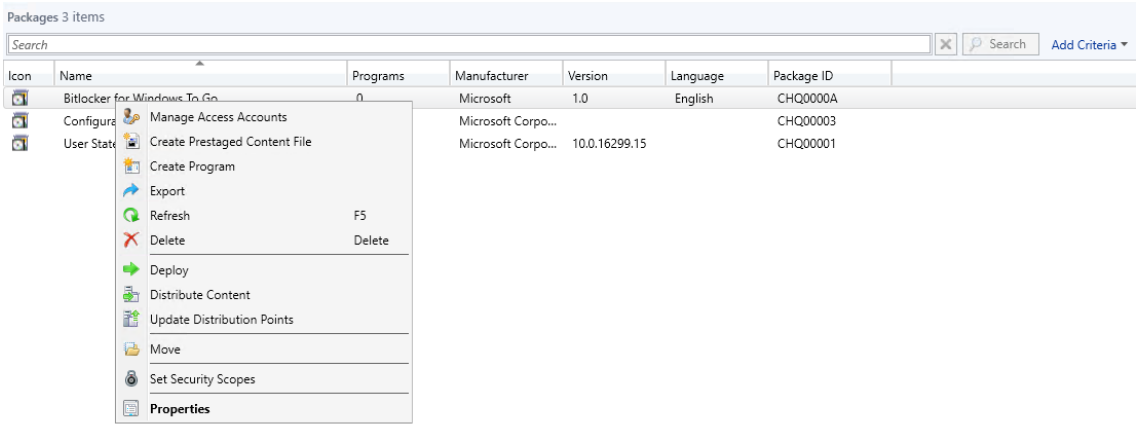
Työkalupaketin luonti aloitetaan, määrittelemällä paketin nimi, sekä yksilöivät tiedot. Lisäksi pakettiin sisällytetään Windows SCCM -palvelimessa oletuksena sisältyvä Bitlocker To Go -asennustyökalu. Valitaan näkymästä valintaruutu ”This package contains source files” ja määritellään työkalun tiedostopolku. Tiedosto löytyy oletuksena sijainnista: \\MicrosoftConfigurationManager\OSD\Tools\WTG\Bitlocker\i386
Kuvassa (Kuva 13) kirjoitetut yksilöivät tiedot, sekä työkalun tiedostosijainti. (Microsoft 2016.)



Kuva 13. Paketin määrittelevät tiedot sekä työkalun tiedostosijainti

Siirrytään seuraavaan vaiheeseen, jossa määritellään paketin sisältö. Työkalun ollessa olemassa, sekä määriteltynä edellisessä vaiheessa, valitaan ”Do not create a program” vaihtoehto. Vaihtoehdolla luodaan paketti, joka sisältää työkalun, sekä mahdollistetaan työkalun jakelu organisaation jakelupisteen kautta.

Summary -sivulla tarkistetaan vielä paketin tiedot ja työkalun oikea tiedostopolku. Tietojen ollessa oikein, valitaan ”Next” ja aloitetaan paketin luominen. Paketin luonnin ollessa valmis, suljetaan paketin luontityökalu. Jotta luotua työkalu pakettia voidaan käyttää asennuksessa, tulee paketti vielä jakaa palvelimen jakelupisteelle. Valitaan luotu paketti hiiren oikealla painikkeella ja jaetaan se jakelupisteille painamalla ”Distribute Content”. Kuvassa (Kuva 14) nähdään avautuva toiminta dialogi, josta valitaan paketin jako.

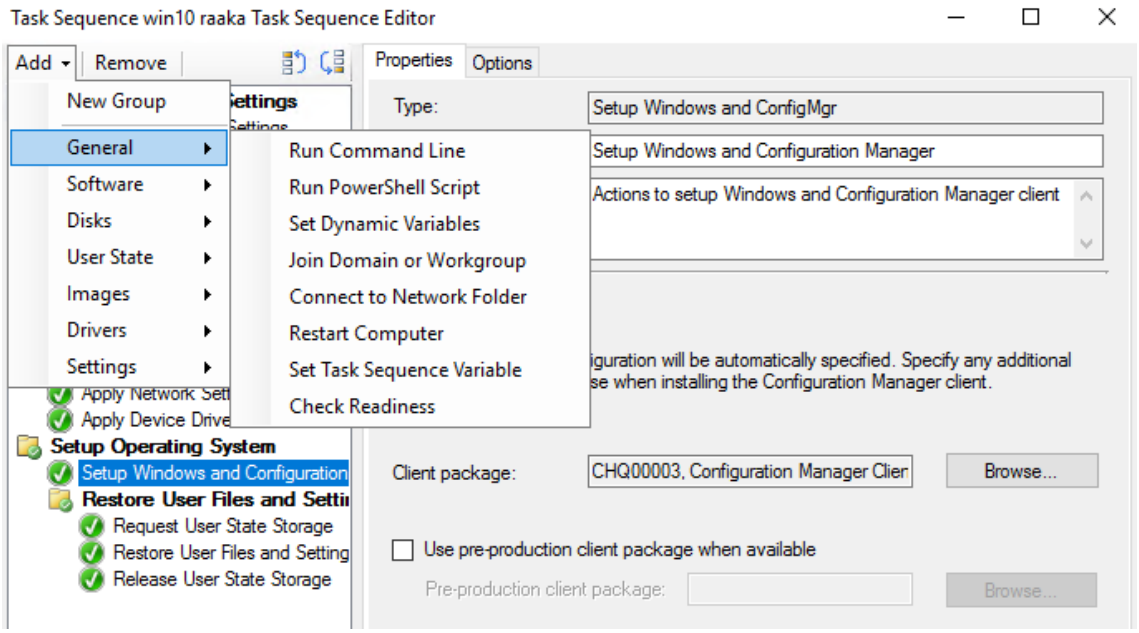


Kuva 14. Luodun työkalun jako tiedostopalvelimelle

Avautuvalla työkalulla määritetään, paketille haluttu jakelupiste. Liittäessä Bitlocker To Go tiedostonsalaus ohjelmaa asennukseen, viitataan määritettyyn jakelupisteeseen, josta SCCM noutaa luodun työkalu paketin.

Seuraavaksi lisätään luotu Bitlocker To Go -asennustyökalu, sekä työkalua kutsuva komentokehoite Task Sequenceen. Avataan ”Task Sequences” sivu ja valitaan aikaisemmin luotu ”Prestaged Media” paketti oikealla hiiren painikkeella. Toiminta dialogista valitaan ”edit”, jolla aikaisemmin luotu paketti avautuu muokkaustilaan.

Muokkaustilassa nähdään asennukseen määritetyt välivaiheet. Lisätään tiedostonsalauksen asentava ominaisuus oikeaan vaiheeseen asennusta, eli käyttöjärjestelmän asennuksen jälkeen. Valitaan listasta kuvassa (Kuva 15) näkyvä ”Setup Windows and Configuration Manager” vaihe. Säännön ollessa maalattuna valitse yläpalkissa sijaitsevasta ”Add” pudotusvalikosta ”General” ja ”Run Command Line” sääntö.



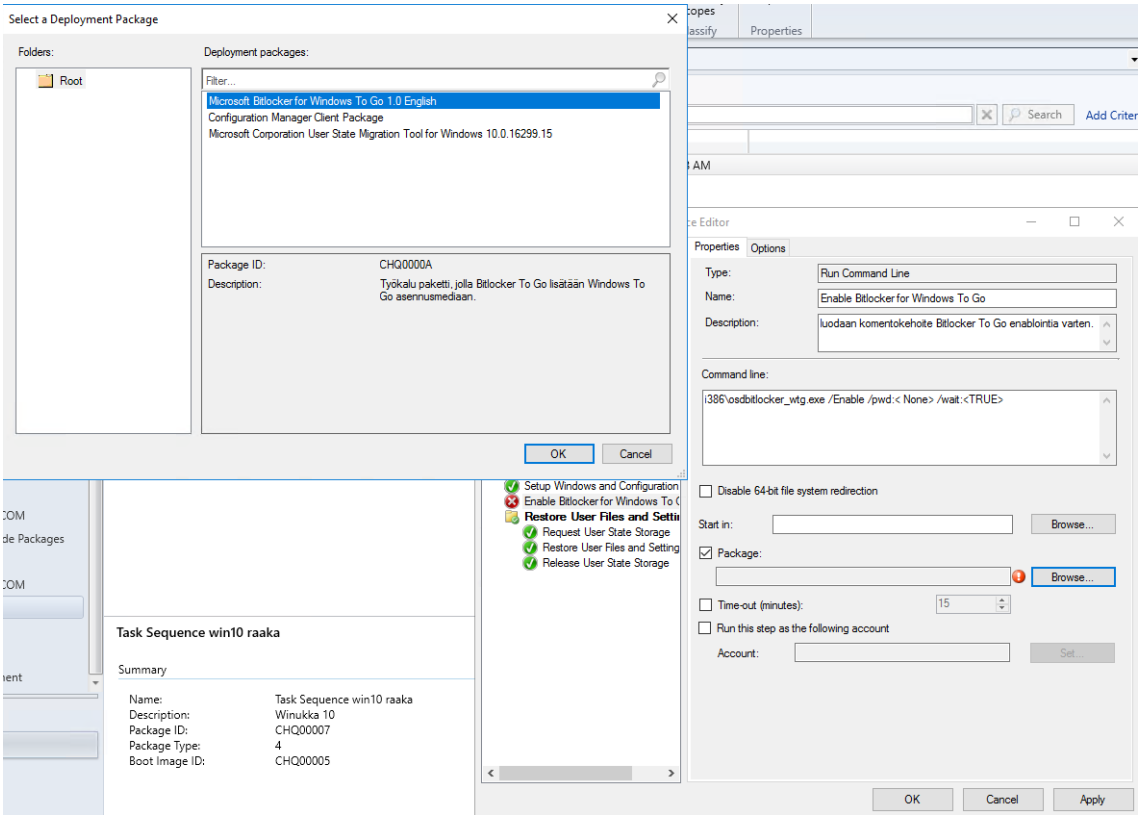
Kuva 15. Task Sequencen muokkaustila, ja säännön lisäys

Properties -välilehdessä nimetään luotu komentorivisääntö helposti tunnistettavalla nimellä, ja kirjoitetaan lyhyt selitys selkoisuutta varten. Komentoriville lisätään komento, jolla asennuksen aikana kutsutaan Bitlocker To Go toimintoa:

```
i386\osdbitlocker_wtg.exe /Enable /pwd:< None> /wait:<TRUE>
```

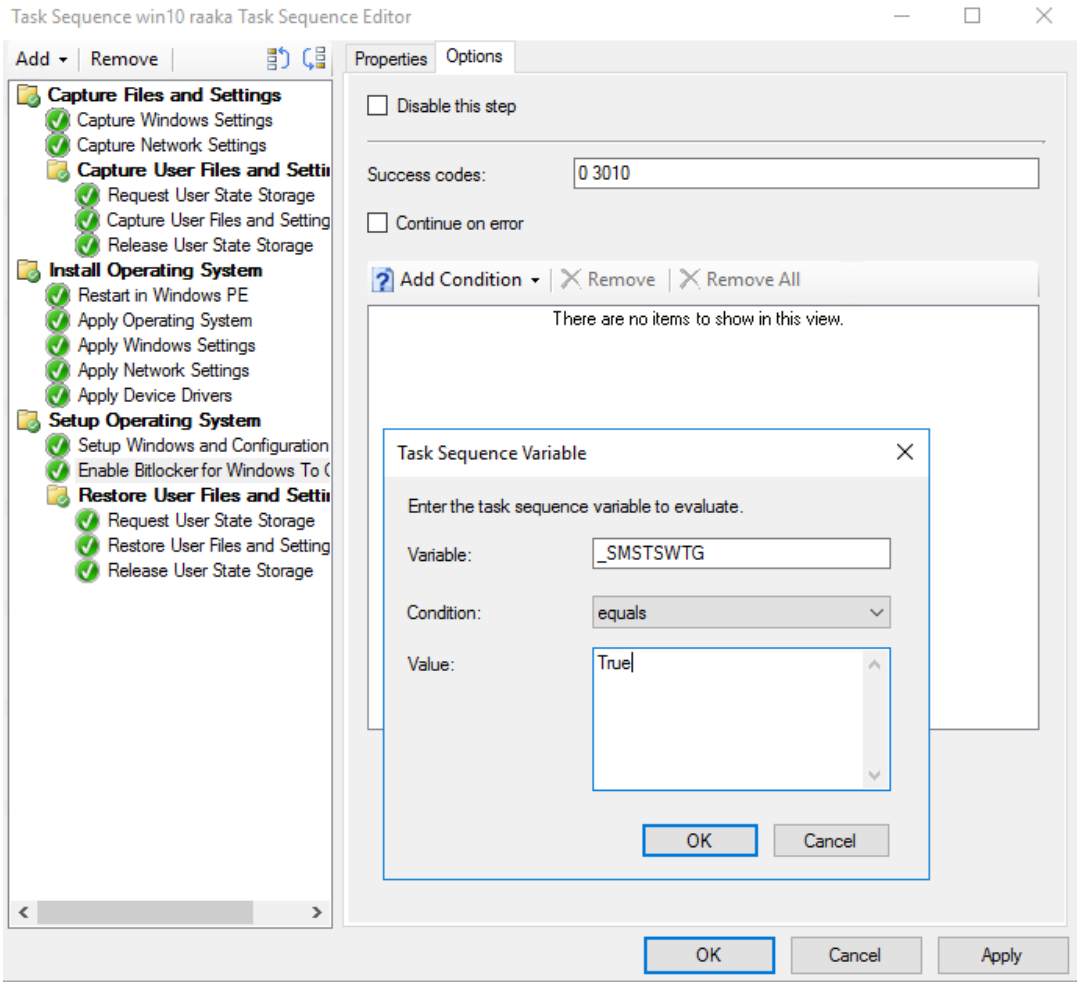
”/pwd:<None|AD>” - määrittelee Bitlocker palautusavaimen sijainnin. Kirjoittamalla ”None” komentoon palautusavain tulee käyttäjälle näkyviin salausavainta määritellessä, josta se tulee ottaa ylös. Mikäli salausavain ja palautusavain unohtuvat käyttäjältä, ei WTG -asemalle pääse.
Kirjoittamalla ”AD” komentoon palautusavain sijoitetaan määritetylle AD DS (Active Directory Domain Services) palvelimelle. Palautusavaimen tallentuessa hallinta palvelimelle voi ylläpito salausavaimen puuttuessa, palauttaa WTG -aseman käyttöön. ”/wait” komennolla määritellään odottaako asennus tiedostonsalauksen valmistumista. Kirjoittamalla sulkeiden sisään ”TRUE” asennus odottaa valmistumista. (Microsoft 2016.)

Komentokehoitteen määrittelyn jälkeen viitataan aiemmassa vaiheessa luotuun ”Bitlocker for Windows To Go” työkalu pakettiin. Mikäli jakelu on onnistunut, tulee paketti näkyviin kuvassa (Kuva 16) näkyvään ikkunaan. Valitaan oikea paketti, jota määritelty komentorivi kutsuu.



Kuva 16. Komentokehoitteen luonti näkymä sekä luotu työkalupaketti

Viimeisessä vaiheessa avataan ”options” -välilehti. Luodaan luodulle komennolle ehto. Ehdon tulee täyttyä, jotta tiedostonsalaus asennus voi edistyä. Avataan ”Add condition” pudotusvalikko ja valitaan ”Task Sequence Variable”. Kirjoitetaan kuvassa (Kuva 17) näkyvät komennot. Muuttujaksi määritellään ”_SMSTSWTG”, jonka tulee olla yhtä kuin ”True”. Kyseisellä muuttujalla varmistetaan, että asennettava asema on Windows To Go -laite. Mikäli ehto ei täyty, komentoriviä ei suoriteta. (Microsoft 2018.)

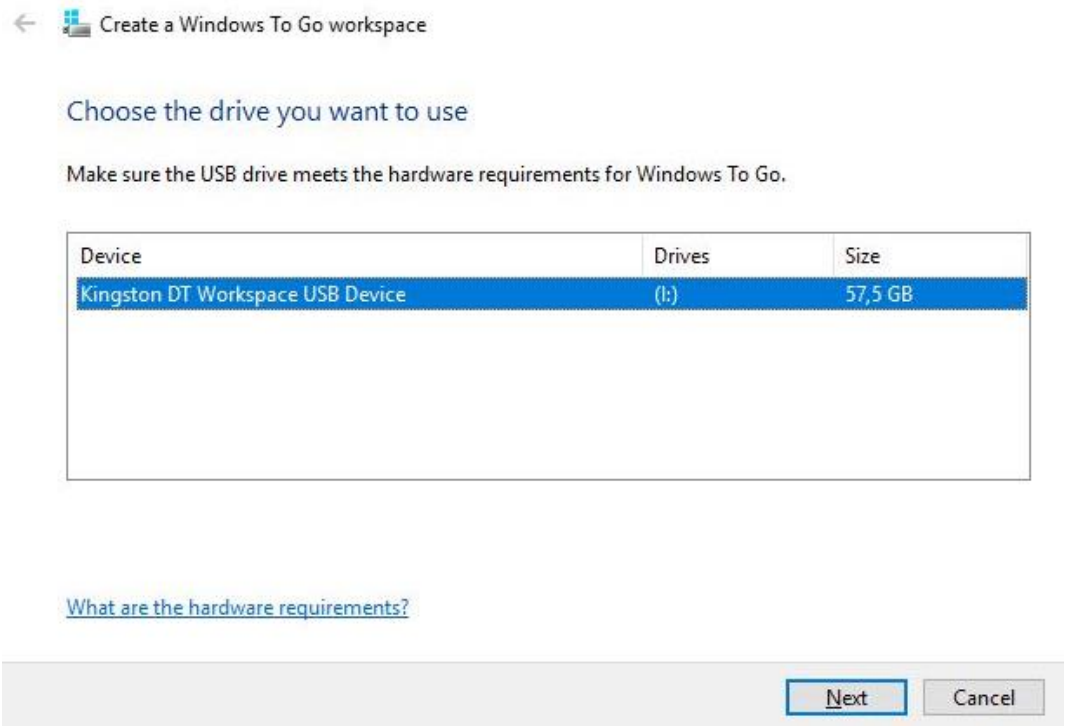


Kuva 17. Ehdon määrittely komentokehoitteelle

Asennuspaketti päivittyy automaattisesti jakelupisteille, sekä tiedosto-sijaintiin tehdyillä muutoksilla. Muutoksen tallentumisen voi vielä tarkistaa painamalla muokattua asennuspakettia. Valitaan alareunassa sijaitsevista välilehdistä ”references” välilehteä, josta voidaan havaita lisätty Bitlocker To Go työkalu. ”Compliance” sarakkeesta huomataan, onnistuiko asennus-paketin lisäys oikein ja onko se yhteensopiva muun asennusmedian kanssa.

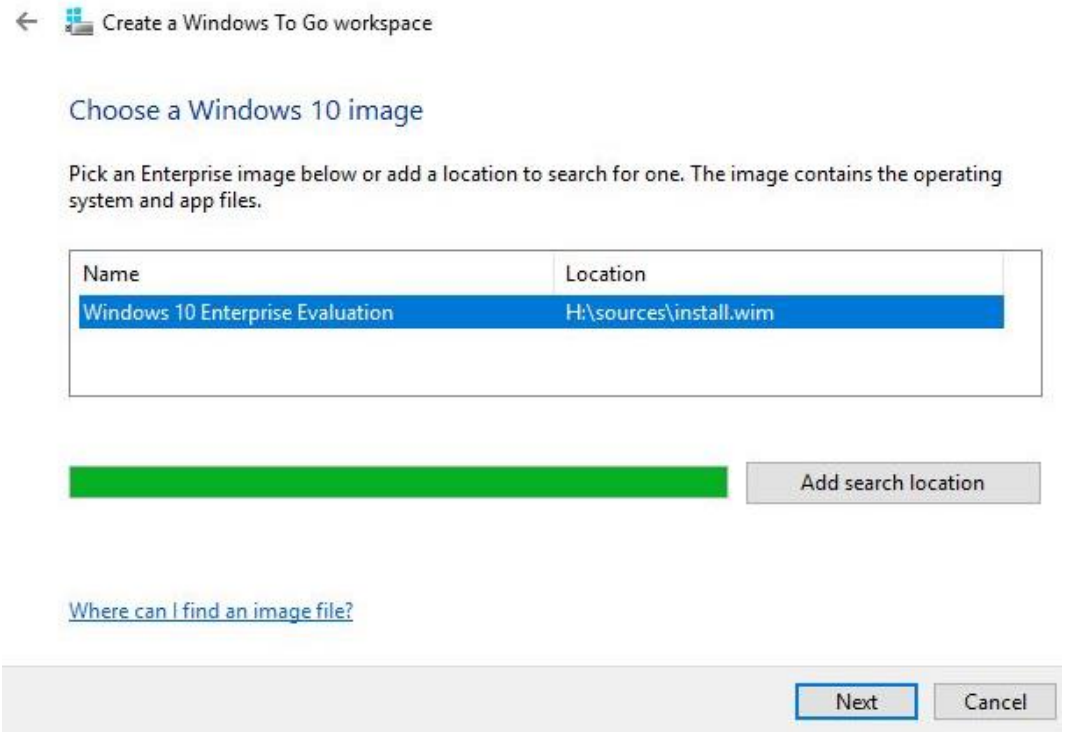
3.2 Windows to Go Creator Wizard

”Windows to Go Creator Wizardilla” luomme WTG-aseman helposti ja no-peasti, mutta ilman muokkausmahdollisuuksia. Liitä sertifioitu WTG USB-muisti koneeseesi mieluiten USB3.0 -porttiin, mutta asennus onnistuu myös USB2.0 -portissa. Haetaan Windows Enterprise ISO tiedosto ja liite-tään se virtuaaliasemaksi, jotta päästään käsiksi install.wim tiedostoon. Avataan Käynnistä valikko ja kirjoitetaan hakuun Windows To Go ja ava-taan asennusohjelma. Kuvassa (Kuva 18) asennustyökalun ensimmäinen ikkuna, jossa valitaan haluttu sertifioitu USB-muisti.



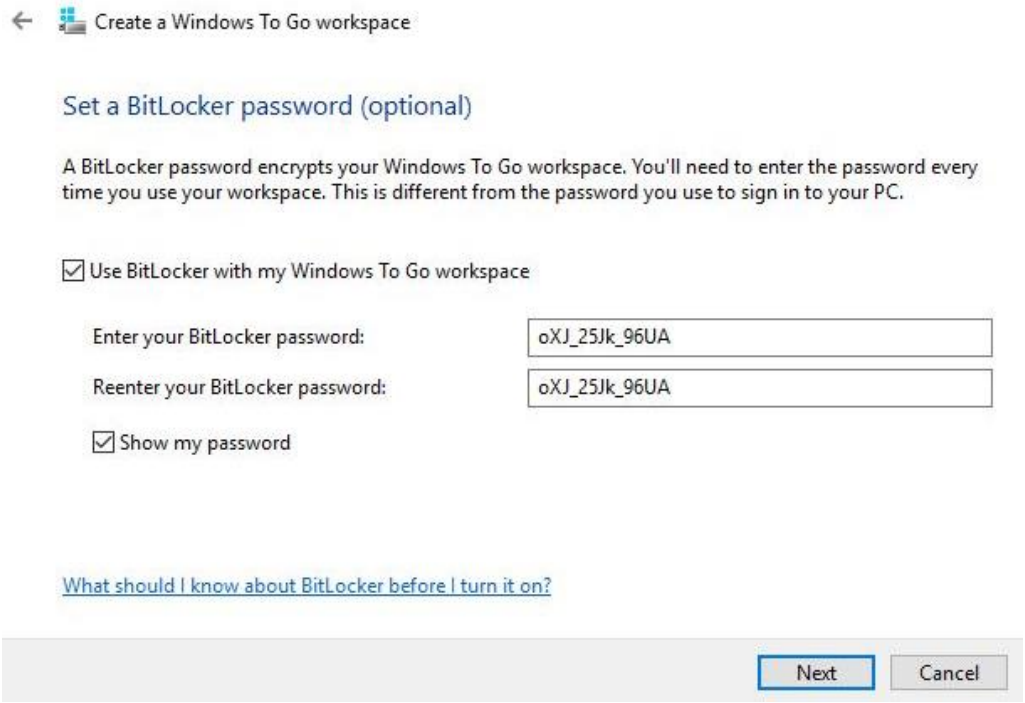
Kuva 18. Sertifioidun USB-muistin valinta

Valitaan alustettu Windows 10 Enterprise -käyttöjärjestelmä näköistiedosto (Kuva 19). Mikäli asennusmedia ei tule heti näkyviin haetaan se painamalla ”add search location” nappia. Täältä navigoidaan .wim tiedoston sijaitsevaan kansioon.



Kuva 19. .wim näköistiedoston valinta

Viimeiseksi valitaan, halutaanko Bitlocker To Go -tiedostonsalaus asettaa päälle (kuva 20). Mikäli käyttöjärjestelmän tiedostonsalausta ei haluta päälle, painetaan alakulmassa sijaitsevaa ohita painiketta. Tiedostonsalauksen saa asetettua päälle myös asennuksen jälkeen Windows asemanhallinta näkymässä. Kirjoita salasanaksi vähintään 8 merkkiä pitkä ja organisaation säädöksiä noudattava salasana. Salasanaa kysytään ennen käyttöjärjestelmän käynnistystä, joten tulee muistaa käyttää vain ASCII merkkejä. Asetetun Bitlocker To Go -tiedostonsalauksen palautusavain tallentuu ylläpitäjäkäyttäjän ”documents” kansioon. Mikäli asennus tehdään koneella, joka käyttää Active Directory Domain Services -asetuksia, tallentuu palautusavain myös AD DS -palvelimelle konetilille, jolla asennus tapahtui. Mikäli WTG USB-muistia aiotaan monistaa tehdyllä asennuksella, asetetaan tiedostonsalaus asennuksen jälkeen ensimmäisellä käyttökerralla. Mikäli tiedoston salausavain on asetettu asennuksen aikana ja tätä monistetaan, pysyy salausavain identtisenä USB-asemissa. Tallentunut palautusavain on myös sama, joka johtaa tietoturvariskiin ja mahdollisiin sekaannuksiin.



Kuva 20. Tiedostonsalauksen asettaminen Windows to Go -työasemalle

Lopuksi varmistetaan vielä, halutaanko Windows To Go -työaseman asennus aloittaa. WTG -työaseman asennus prosessi kestää 10-30 minuuttia ja näet edistymisen ruudulla olevasta palkista. Valmistumisikkuna tulee näkyviin ja ilmoittaa kun WTG -työaseman on valmis käytettäväksi. Voit nyt asettaa WTG käynnistys asetuksen päälle ja uudelleen käynnistää luodulle työasemalle.

3.3 Windows PowerShell

PowerShell komentotulkki ohjelmalla asennus luodaan manuaalisesti käyttäen komentosarjoja. PowerShell -komentosarjoilla voidaan USB-asema luoda automatisoidusti tukien moniajoasennusta merkittävillä muokkausmahdollisuuksilla.

Windows PowerShell avataan ylläpitäjätilassa, kirjoittamalla Windows hakuun PowerShell ja klikkaamalla oikealla hiiren painikkeella ”avaa admin tilassa”. Kirjoitetaan komentoriville ”get-disk” komento, jolla näemme, löytyykö Windows To Go -asennusta varten oleva USB-asema. Kuvasta (Kuva 21) näemme WTG -sertifioidun USB-aseman, Kingston DT Workspace ja tarkistamme tämän levyaseman numeron, joka on tässä tapauksessa neljä. (Microsoft 2015.)

```
PS C:\Users\Joni> get-disk

Number Friendly Name                 Serial Number                HealthStatus         OperationalStatus      Total Size Partition
                                                                                                                         Style
------ -------------                 -------------                ------------         -----------------      ---------- ---------
3      Samsung SSD 960 EVO 500GB     0025_385B_71B0_31B8.         Healthy              Online                  465.76 GB GPT
1      SAMSUNG HD103SI               S1VSJ90SB59946               Healthy              Online                  931.51 GB MBR
0      Samsung SSD 850 PRO 256GB     S251NSAG529994Z              Healthy              Online                  238.47 GB MBR
2      WDC WD5000AAKX-00ERMA0             WD-WMC2E0494247         Healthy              Online                  465.76 GB MBR
4      Kingston DT Workspace         302E26080G21D2FC00C4         Healthy              Online                    57.6 GB MBR
```

Kuva 21. Windows To Go -muistin levyaseman numeron haku

Suoritetaan sertifioidulle Windows To Go USB-asemalle formatointi, jolla poistamme asemalta edelliset tiedot sekä partitiot (Kuva 22). Mikäli USB-asema on ollut aikaisemmin käytössä, saadaan näin poistettua edellisen käyttäjän kaikki tiedot. Syötämme komentoriville komennot:

```
Clear-Disk $DiskNumber –RemoveData –RemoveOEM –
Confirm: $False
Get-Disk $DiskNumber | Get-Partition | Remove-Par-
tition –confirm: $False
```

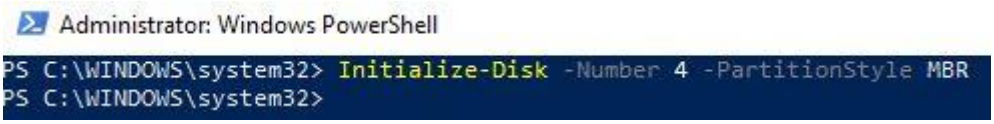
(Microsoft 2015.)

```
Clear-Disk 4 -RemoveData -RemoveOEM -Confirm:$False
   1/2 completed
   [oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo                    ]
   00:00:00 remaining.
  Clearing disk
     Running
     [                                                                              ]

Number Friendly Name Serial Number                HealthStatus         OperationalStatus      Total Size Partition
                                                                                                         Style
------ ------------- -------------                ------------         -----------------      ---------- ---------
3      Samsung SS... 0025_385B_71B0_31B8.         Healthy              Online                  465.76 GB GPT
1      SAMSUNG HD... S1VSJ90SB59946               Healthy              Online                  931.51 GB MBR
0      Samsung SS... S251NSAG529994Z              Healthy              Online                  238.47 GB MBR
2      WDC WD5000...      WD-WMC2E0494247         Healthy              Online                  465.76 GB MBR
4      Kingston D... 302E26080G21D2FC00C4         Healthy              Online                    57.6 GB RAW


PS C:\WINDOWS\system32> Get-Disk 4 | Get-Partition | Remove-Partition -confirm:$False
PS C:\WINDOWS\system32> Clear-Disk 4 -RemoveData -RemoveOEM -Confirm:$False
```

Kuva 22. Windows To Go -muistin formatoinnin edistymisen seuranta

Formatoinnin jälkeen USB-asema tulee partitioida uudelleen. Kirjoitamme komentoriville alustus Cmdlet komennon (Kuva 23), jolla alustamme aseman uudelleen partitiointia varten. Kirjoitetaan komentoriville komennot:

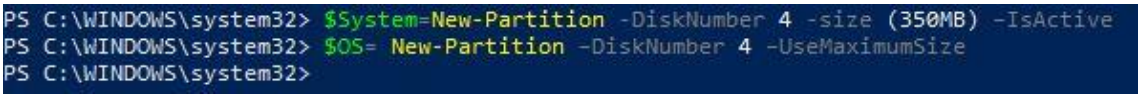
```
Initialize-Disk –Number $DiskNumber –Parti-
tionStyle MBR
```
(Microsoft 2015.)



Kuva 23. Windows to Go -muistin alustus

Luodaan USB-asemalle kaksi eri partitiointia (Kuva 24). Ensimmäinen partitiointi on 350 mb kokoinen järjestelmä partitio, jolle tarvittavat asennustiedostot sijoitetaan (Windows Preinstallation Environment). Loput tilasta jätämme käyttöjärjestelmälle ja halutuille tiedostoille. Loppu partition koko on siis tässä tapauksessa 57,2 gb. Vaikka kyseessä on 64 gb kokoinen USB-asema on WTG -sertifioiduissa asemissa niin sanottu ”piilotettu partitio”, jossa on tarvittavat mediat automaattista ajuri tunnistusta varten. Kirjoitetaan komentoriville komennot:

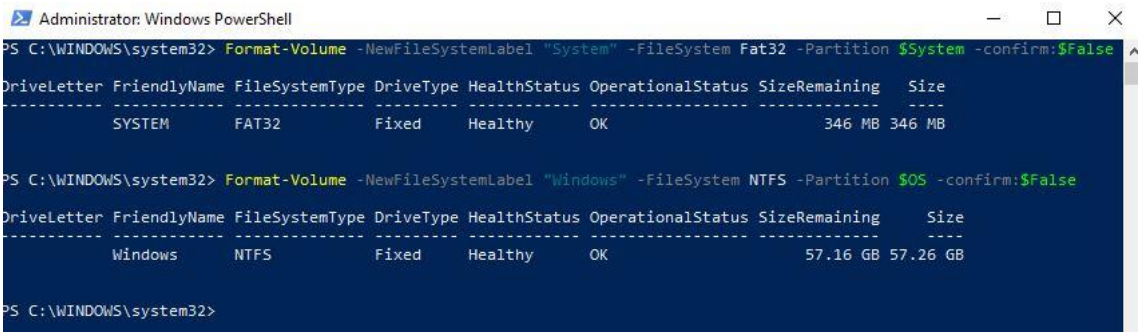
```
$System=New-Partition –DiskNumber $DiskNumber –
size (350MB) –IsActive
$OS= New-Partition –DiskNumber $DiskNumber –Use-
MaximumSize
```
(Microsoft 2015.)



Kuva 24. Partitio komennot työasemalle

Seuraavassa vaiheessa luomme juuri tehdyille partitioille asematunnukset ja tiedostojärjestelmä muodot (Kuva 25), jotka tässä tapauksessa ovat asennustiedostoille FAT32, käyttöjärjestelmälle sekä tiedostoille NTFS. Kirjoitetaan komentoriville komennot:

```
Format-Volume -NewFileSystemLabel "System" –
FileSystem FAT32 –Partition $System –confirm:
$False
Format-Volume -NewFileSystemLabel "Windows" –
FileSystem NTFS –Partition $OS –confirm: $False
```
(Microsoft 2015.)



Kuva 25. Valmiit partitiot PowerShell näkymässä

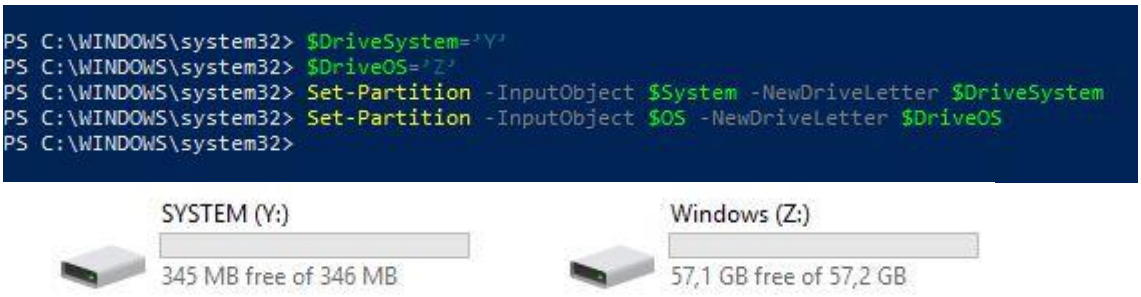
Annetaan partitioille asematunnukset, kuten tässä tapauksessa asemat nimetään Y:ksi ja Z:ksi. Ensiksi luodaan DriveSystem Y ja DriveOS Z nimeäjät kirjoittamalla komentoriville komennot:

```
$DriveSystem='Y'

$DriveOS='Z'
```

Viitataan luodut nimeäjät oikeille partitioille (Kuva 26) kirjoittamalla komentoriville komennot:

```
Set-Partition -InputObject $System -NewDriveLetter $DriveSystem
Set-Partition -InputObject $OS -NewDriveLetter $DriveOS
```

(Microsoft 2015.)



Kuva 26. Asemien nimeäminen ja tiedostonäkymä asemista

Yksi tärkeimmistä Windows To Go -toiminnallisuuden ominaisuuksista on se, että mikäli asema yhdistetään tietokoneeseen ja sitä lukee vieras käyttöjärjestelmä, se ei saa asematunnusta jolloin tätä ei voida lukea ja tiedostot säilyvät turvassa. Lisäämme nyt tämän toiminnon asemalle komennolla.

```
Set-Partition -InputObject $OS –NoDefaultDriveLetter
```

Seuraavassa vaiheessa asennusta asetamme USB-asemalle Windows -käyttöjärjestelmän. Näköistiedosto voi olla muokkaamaton .wim Windows

tiedosto tai esim. SDK:lla tai SCCM:llä kasattu, räätälöity .wim tiedosto. WIM (Windows Imaging Format) on tiedostopohjainen levy formaatti, joka sisältää käyttöjärjestelmään vaadittavia tiedostoja ja tiedostojärjestelmän metadatan. (Microsoft 2017.)

Näköistiedoston asennuksessa on kolme eri vaihetta:

- Näköistiedoston asennus USB-asemalle
- Windows To Go USB-aseman asettaminen bootti mediaksi
- Pääsyoikeuksien rajoittaminen luoduille järjestelmä partitioille SAN policy konfiguroinnilla

Näköistiedoston asettamiseksi käytämme Expand-WindowsImage CMDlettiä, joka ajaa saman asian kuin DISM.exe, mutta etu edellä mainitussa komennossa on sen johdonmukaisuus parametreissä. (Microsoft 2015.)

CMDlet:llä määrittelemme polun .wim näköistiedostoon, indeksi numeron, joka selvitettiin alussa get-disk komennolla, ja asennettava sijainti.

System partitio ja DriveOS partitio nimettiin alussa Y ja Z nimisiksi, mutta tässä vaiheessa DriveOS partitio muutetaan C: muotoon. Kirjoitetaan siis komentoriville komento, jolla formatoidaan aikaisemmin annettu tunnus ja Windows nimeää sen oletus muotoon:

```
$DriveOS':
```

Tämän jälkeen ajetaan komentorivillä Expand-WindowsImage komento:

```
$Wimfile='.\install.wim'
Expand-WindowsImage –imagepath "$wimfile" –index 1
–ApplyPath "$DriveOS`:\"
```
(Microsoft 2015.)

Näköistiedoston toimiessa PowerShell -komentoikkunaan ilmestyy asennuksen edistymistä kuvaava palkki. Palkki näyttää vain asennuksen aloituksen ja valmistumisen. USB-aseman ollessa USB3.0 portissa käyttöjärjestelmän asennus kestää noin 10 minuuttia. Mikäli vain USB2.0 portti on käytössä, asennuksessa kuluu noin 15-30 minuuttia.

Tämän jälkeen ajetaan BCDBoot komento Windowsissa, jotta bootti asetukset asentuvat tikulle. BCDBoot on Windows komentorivi työkalu, jolla asennetaan käynnistysominaisuus asemalle ja määritellään käynnistysasetukset. BCDBoot komennon sisältävä komento haetaan käyttämällä $ENV:Windir muuttujaa. Kirjoitetaan komento, jolla työkalu haetaan ja sijoitetaan USB-asemalle:

```
&"$($env:windir)\system32\bcdboot"          "$Driv-
eOS`:\Windows" /f ALL /s "$Systemdrive`:"
```

(Microsoft 2015.)

Seuraavaksi luodaan asennukselle Unattend.xml tiedosto ”Sysprep” kansioon WTG -muistiin. Käynnistettäessä käyttöjärjestelmä prosessoi kyseisen tiedoston ja asettaa tehdyt komennot tiedostosta voimaan. Unattend.xml tiedostolla määritellään työaseman perus konfiguraatiot. Toimii samalla periaatteella kuin myöhemmin tehtävä SAN-Policy.xml tiedosto, sillä erolla, että siihen tarvitsee nimetä muutaman muuttujan arvon, kuten työaseman nimen. (Microsoft 2015.)

Tässä tapauksessa teemme yksinkertaisen Unattend.xml tiedoston (Kuva 27), johon määrittelemme aikavyöhykkeen, työaseman nimen (WTG-numeerinen muuttuja), organisaation nimen, hallinnointi salasanan sekä haltijan. Kirjoitetaan Unattend.xml tiedosto esimerkiksi Notepad+ ohjelmalla ja tallennetaan se helposti saavutettavaan sijaintiin.

Unattend - Notepad

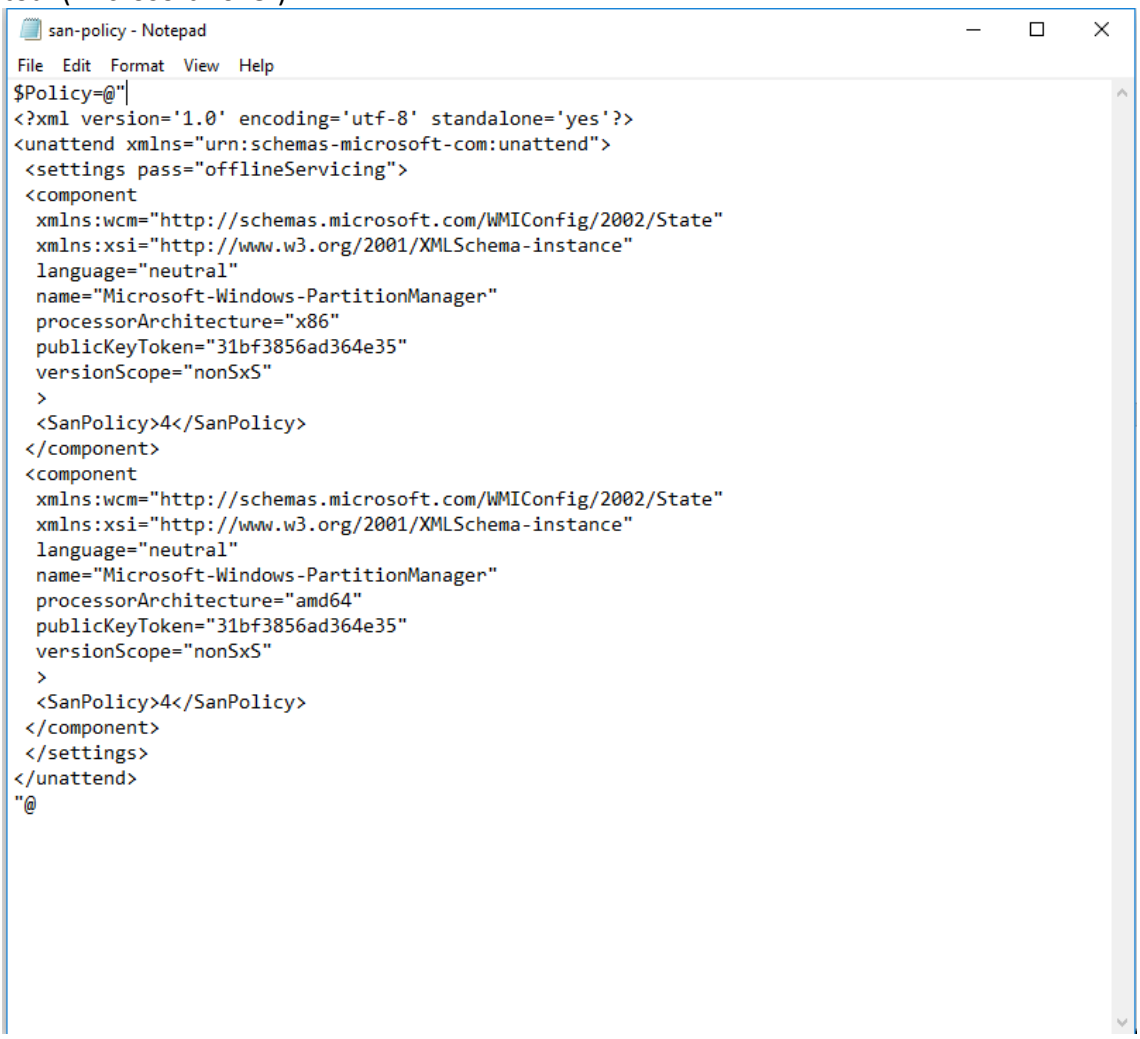
File Edit Format View Help

```
$Computername=”WTG-$(Get-Random)”
$Organization=’PVTUTKL’
$Owner=’PVTUTKL RMK’
$Timezone=’FLE Standard Time’
$AdminPassword=’HRVU3py3R’
$Unattend=@"
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
 <settings pass="specialize">
  <component name="Microsoft-Windows-Shell-Setup" processorArchitec-ture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <ComputerName>$Computername</ComputerName>
   <RegisteredOrganization>$Organization</RegisteredOrganization>
   <RegisteredOwner>$Owner</RegisteredOwner>
   <TimeZone>$Timezone</TimeZone>
  </component>
 </settings>
 <settings pass="oobeSystem">
  <component name="Microsoft-Windows-Shell-Setup" processorArchitec-ture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <UserAccounts>
    <AdministratorPassword>
     <Value>$Adminpassword</Value>
     <PlainText>true</PlainText>
    </AdministratorPassword>
   </UserAccounts>
              <AutoLogon>
               <Password>
                <Value>$Adminpassword</Value>
                <PlainText>true</PlainText>
               </Password>
              <Username>administrator</Username>
              <LogonCount>1</Log\onCount>
              <Enabled>true</Enabled>
              </AutoLogon>
   <RegisteredOrganization>$Organization</RegisteredOrganization>
   <RegisteredOwner>$Owner</RegisteredOwner>
   <OOBE>
    <HideEULAPage>true</HideEULAPage>
    <SkipMachineOOBE>true</SkipMachineOOBE>
   </OOBE>
  </component>
 </settings>
 <cpi:offlineImage cpi:source="" xmlns:cpi="urn:schemas-microsoft-com:cpi" />
</unattend>
"@
```

Kuva 27. Unattend.xml määritys tiedosto

Unattend.xml tiedoston ollessa valmis tallennetaan tai siirretään se ”Sysprep” kansioon Windows To Go asemalle.

Asetetaan asennukselle SAN-Policy.xml tekstitiedosto. Tekstitiedosto määrittelee mitä tapahtuu asemille liityttäessä isäntäkoneeseen eli tikun kiinnittyessä tai käynnistyessä. Oletus konfiguraatiolla San Policy "4" Windows To Go jättää kaikki isäntäkoneen asemat offline tilaan. Oletuskonfiguraatiolla piilotetaan myös WTG USB-asema. Mikäli WTG -asema liitetään isäntäkoneeseen tämän ollessa käynnissä, ei asemalle ole määritelty asematunnusta. Asema pysyy siis offline-tilassa ja ei näin ollen näy tiedostojärjestelmänä. SAN-Policy.xml (Kuva 28) tiedosto voidaankin siis muokata tarpeita palvelevaksi, mutta esimerkissä käytetään normaalia oletustiedostoa. (Microsoft 2015.)



Kuva 28. San-policy.xml määritys tiedosto

Remove-Item ja Add-Content komennoilla voidaan muokata SAN-Policy.xml tiedostoa. Tässä tapauksessa haluamme muuttaa kyseistä tiedostoa niin että muokkaamme komennon -erroraction, jotta asennus ei keskeydy virheen sattuessa. Kirjoitetaan komentoriville komento:

```
$SanPolicyFile='.\san-policy.xml'
```

```
Remove-item $SanPolicyFile -erroraction Silently-
Continue

Add-content -path $SanPolicyFile -Value $Policy
```
(Microsoft 2015.)

Lopuksi ajetaan vielä Use-WindowsUnattend cmdlet, joka ajaa aikaisemmin määritellyt asetukset Unattend.xml tiedostosta. Kyseiselle komennolle tulee antaa käyttöjärjestelmän asema nimike ja luodun SAN-Policy.xml tiedoston nimi. Kirjoitetaan komentoriville komento:

```
Use-WindowsUnattend –unattendpath $SanPolicyFile –
path "$DriveOS`:\"
```
(Microsoft 2015.)

Windows To Go USB-asema on nyt valmis käynnistettäväksi. Asemalla on aikaisemmin määritellyt asetukset ja bootti ominaisuudet.

4 ETÄHALLINTA JA PÄIVITTÄMINEN

Varmistaaksemme, että Windows To Go -työasemat ovat mahdollisen käytännöllisiä muualla kuin organisaation toimitiloissa on onnistuneella etähallinnalla suuri merkitys. Yksi tämän päivän merkittävimmistä organisaatio toiminnallisuuksista onkin mahdollisuus antaa käyttäjien käyttää organisaation hallinnoimaa toimialuetta etänä, samoin kuin paikan päällä toimistolla. Turvallinen etäyhteystekniikka mahdollistaa etäkäyttäjän turvallisen pääsyn yrityksen tietoresursseihin.

WTG -asemaa luodessamme, joko ”PowerShellillä” tai ”Microsoft SCCM:llä” voimme asennuksen konfiguraatioita muuttamalla liittää aseman suoraan toimialueelle. Asemien näin ollessa organisaation toimialueella voidaan mm. Group Policy -säännöillä helposti hallita etätyöasemien rajoituksia tai ”Microsoft SCCM -hallinnoinnilla” tuoda tärkeitä päivityksiä sekä ohjelmia käyttäjälle. Etäyhteystekniikoina toimivat Direct Access sekä VPN (Virtual Private Network), jotka mahdollistavat turvallisen tavan etätyöskentelyyn.

4.1 **Direct Access**

Direct Access -toiminto mahdollistaa automaattisen yhteyden muodostuksen yrityksen verkkoon MS-IPHTTPS (Microsoft IP over HTTPS Tunneling Protocol) tunnelointiprotokollalla. Yhteyden muodostaminen alkaa välittömästi asiakaskoneen kytkeydyttyä verkkoon, eikä yhteyden muodostaminen sisäverkkoon vaadi erillistä sisäänkirjautumista. Koska Direct Access pysyy aina aktivoituna, ei käyttäjältä vaadita erillisiä toimenpiteitä. Siitä lähtien, kun organisaation intraverkko on yhteydessä Direct Access -käyttäjäohjelmaan verkkoyhteyden toimiessa, hallinta agentit voivat kommunikoida intraverkon palvelimen kanssa saaden päivityksiä ja raportteja. Tämä tarkoittaa myös sitä, että Direct Access -käyttäjät saavat säännöllisesti Group Policy -päivitykset. Direct Access yhteyden avulla voidaan myös ottaa etätyöpöytä yhteys käyttäjään mahdollisia tukipyyntöjä varten.
(Richard M. Hicks Consulting, Inc. 2012.)

Direct Access tekniikkaa käyttääksesi tarvitset:

- Windows 10 Enterprise käyttöjärjestelmän.
- IPv6 IP-protokollalla toimivan verkon.
- Toimialueeseen liitetyn isäntäkoneen, jolla WTG asennus tapahtuu.
- WTG-aseman, jota ei ole käynnistetty tai liitetty toimialueeseen käyttämällä unattend asetuksia.
- Käyttäjätilin, jolla voidaan lisätä työasemia toimialueelle sekä ylläpitäjän oikeudet työasemalle, jolla WTG-asema tehdään.
- Aktiiviseksi konfiguroidun Direct Accessin toimialueella.

(Microsoft 2017.)

Direct Access konfigurointi aloitetaan WTG-asemalle käynnistämällä isäntäkone, jolla asennus tapahtuu. Koneelle kirjaudutaan tunnuksilla, joilla on oikeus lisätä työasemia toimialueelle ja avataan komentokehote työkalu ylläpitäjä tilassa ja syötä seuraava komento:

```
djoin /provision /domain <exampledomain.com> /machine <examplewindowstogo_workspace_name> /certtemplate <WorkstationAuthentication_template> /policynames <DirectAccess Client Policy: {GUID}> /savefile <C:\example\path\domainmetadatafile> /reuse
```

< > Sulkujen sisällä esimerkki parametrit, jotka muutetaan organisaation toimialueelle sopiviksi. (Microsoft 2017.)

Tämän jälkeen liitetään Windows To Go -asema työasemaan kiinni ja tehdään aiemmin mainituin PowerShell ohjein asennus. Asennuksen tultua pisteeseen, jossa teemme unattend.xml tiedoston syötämme komennon `djoin /requestodj /loadfile C:\example\path\domainmetadatafile /windowspath W:\Windows`
, jolla haemme aikaisemmin luodun domain metadatan. Tämän jälkeen muokkaamme unattend.xml tiedostoa sijoittamalla <OOBE> parametrien

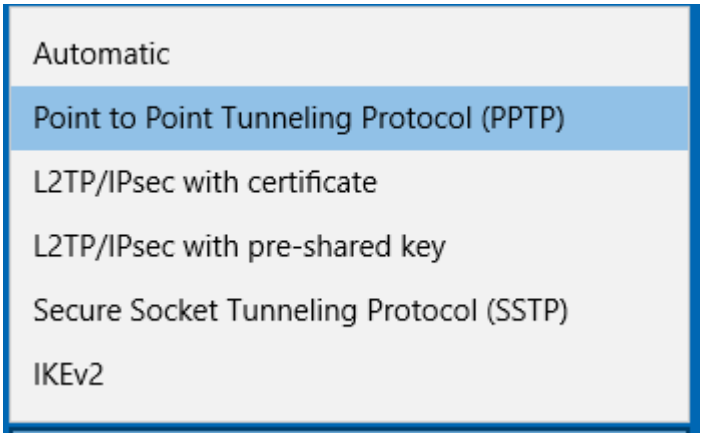
sisään komennon <NetworkLocation>Work</NetworkLocation>, jolla asemalle kerrotaan sen olevan osa organisaation yksityistä toimialuetta. Suorita asennus loppuun ja irrota WTG-asema koneesta. Käynnistettäessä WTG -asema tulisi olla organisaation toimialueella, mikäli yhteys intraverkkoon toimii. (Microsoft 2017.)

4.2 **VPN**

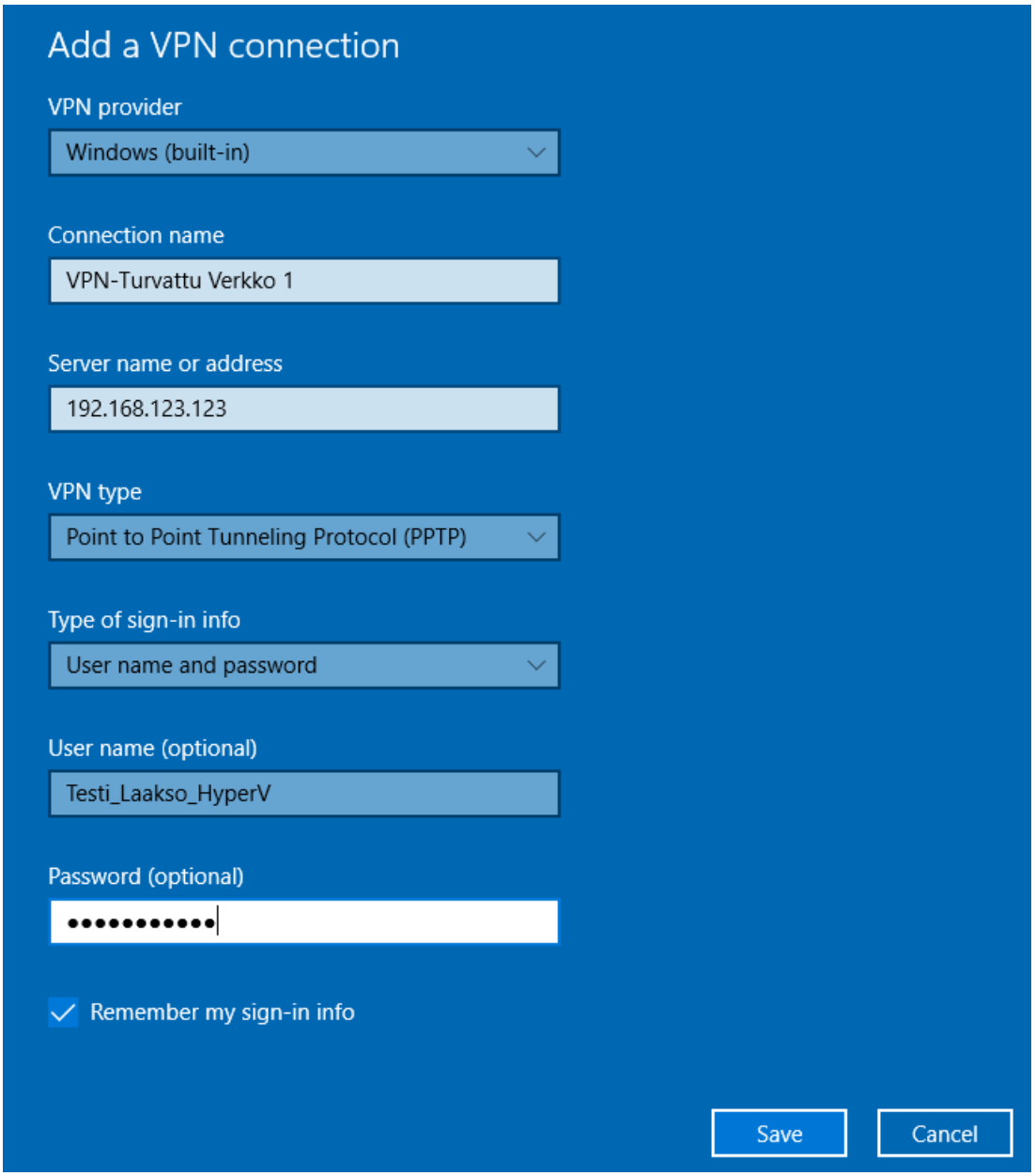
VPN (Virtual Private Network) eli virtuaalinen erillisverkko mahdollistaa turvallisen etäyhteyden organisaation lähiverkkoon julkisen verkon yli. VPN mahdollistaa organisaation työntekijöille varsin turvallisen tavan etätyöskentelyyn mistäpäin tahansa toimiston ulkopuolelta ja pääsyn organisaation järjestelmiin, kuten sähköpostiin, tietokantoihin, tulostimiin sekä dokumentteihin. VPN-ratkaisun turvallisuus perustuu tunnelointitekniikkaan etäyhteyttä muodostettaessa. Kahden pisteen välinen yhteys salataan erityisellä tunnelointiprotokollalla kuten Point- to- Point Tunneling Protocol (PPTP), sekä autentikointiprotokolalla kuten PAP. Yhteyden tunneloinnilla salataan siis kahden tai useamman pisteen välinen dataliikenne ulkopuolisilta ja yhteyden autentikoinnilla varmistetaan VPN-yhteyden osapuolet oikeaksi. (Ballew 2016, 102.)

VPN asetuksia ei ole mahdollista konfiguroida Windows To Go -asemalle asennuksen yhteydessä. Etäyhteyden ottaminen VPN:n avulla tapahtuu käyttäjän toimesta käynnistyksen jälkeen. Yhteyden muodostaminen aloitetaan luomalla VPN-profiili itsellesi. Voit luoda VPN-profiilin itse tai määrittää työtilin, johon liität organisaatioltasi saamasi VPN-profiilin.

Valitse Aloita-painike ja sitten Asetukset-valikko. Asetukset -valikosta siirry Verkko ja Internet, jonka jälkeen vasemmasta ruudun reunasta VPN, lisää VPN-yhteys. Lisää VPN-yhteys -kohdassa tee seuraavat organisaatiosi ohjeiden mukaiset asetukset. Valitse VPN-verkon tarjoa -kohdassa Windows (sisäinen). Kirjoita Yhteyden nimi -ruutuun haluamasi helposti tunnistettava nimi, josta tunnistat VPN-yhteyden, johon haluat muodostaa yhteyden. Palvelin nimi tai Osoite -kohtaan kirjoita organisaatiosi VPN-palvelimen yhteysosoite, eli IP-osoite tai web-osoite. VPN-tyyppi ruudussa valitse organisaatiosi käyttämä yhteysprotokolla (Kuva 29). Valitse Kirjautumistietojen tyyppi -kentässä organisaatiosi kirjautumistapa, kuten älykortti, varmenne tai käyttäjänimi ja salasana. Lopuksi valitse tallenna. Kuvasta (Kuva 30) näemme esimerkin täytetystä VPN-yhteys profiilista.

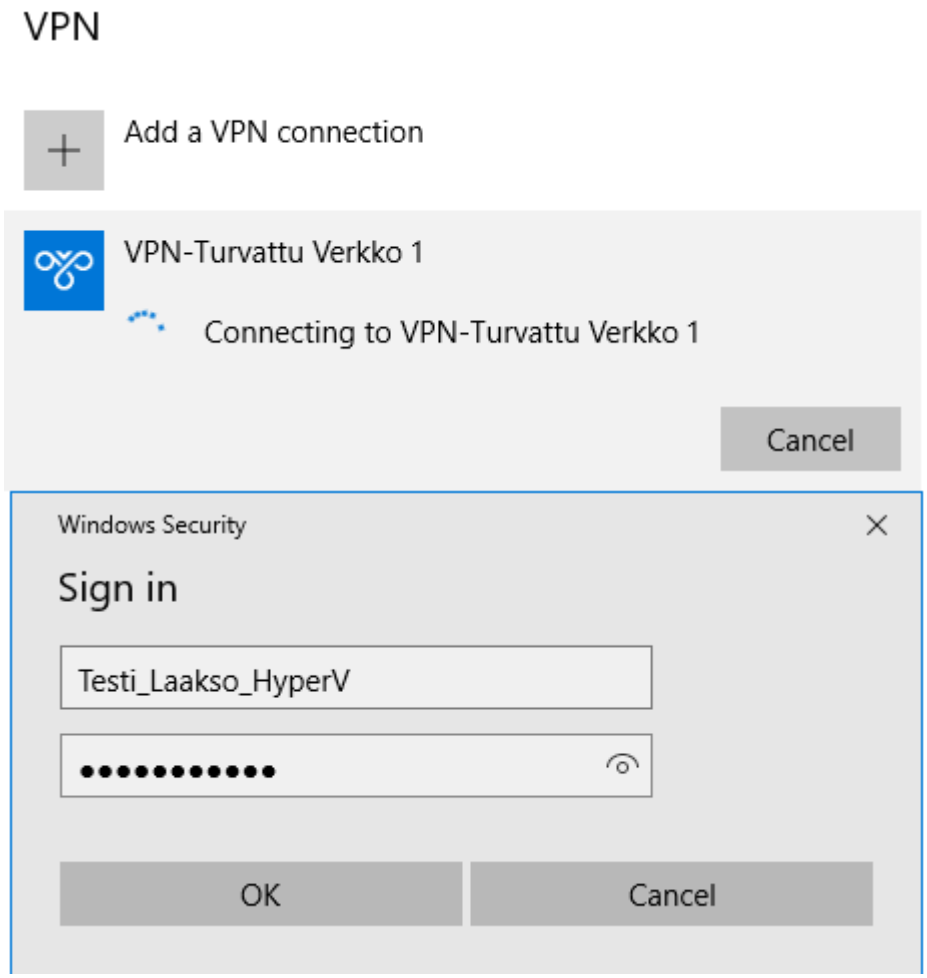


Kuva 29. yhteysprotokolla valinta



Kuva 30. VPN-yhteyden määrittely

Kun olet tehnyt VPN-profiilin, voit muodostaa yhteyden organisaatiosi turvattuun verkkoon. Valitse tehtäväpalkin oikeasta reunasta Verkko-kuvakkeesta tai Aloita -valikosta, Asetukset ja täältä Verkko ja Internet, josta valitsemme VPN-alavalikon. Valitaan aikaisemmin tehty VPN-yhteys ja painetaan yhdistä-painiketta. Organisaatiosi sisäänkirjautumistavastasi riippuen anna käyttäjänimesi ja salasanasi tai muut kirjautumistiedot. Kuvassa (Kuva 31) esimerkki VPN-yhteys kirjautumisruudusta. Kun yhteys on muodostettu VPN-palvelimeen, lukee verkon nimen alapuolella yhdistetty. Voit tarkistaa VPN-yhteyden myös tehtäväpalkin oikeassa alareunassa sijaitsevasta Verkko-kuvakkeesta.



Kuva 31. Kirjautuminen määriteltyyn VPN-tunneliin

Windows 10 1607 päivityksen mukana esitelty uusi VPN -arkkitehtuuri Always On VPN toimii samalla periaatteella, kuin Direct Access. Koneen yhdistyessä verkkoon, kirjautuu se automaattisesti organisaation intraverkkoon mahdollistaen käyttäjän turvallisen yhteyden organisaation resursseihin. Direct Access toiminnosta eroten Always On VPN käyttää vanhan VPN version tavoin IKEv2, SSTP, L2TP ja PPTP protokollia ja täten käyttää edestakaiseen kommunikointiin dual stack tekniikkaa eli IPv4 tai IPv6 osoitteita. Kun Direct Access vaatii toimialueeseen liitetyn Enterprise tai Education -käyttöjärjestelmä version toimii Always On VPN myös muissa versi-

oissa, eikä näiden tarvitse olla toimialueella. Tällä hetkellä (Windows versio 1709) Always On VPN vaatii käyttäjä konfigurointiin PowerShell, SCCM, tai Intune hallinnoinnin. (4sysops 2017.)

4.3 **Windows Update**

Windows To Go -työaseman päivitys tapahtuu samoin kuin perinteisenkin työaseman. Laitteen tullessa internet käyttöön, asemalle ei määritellä toimialuetta, joten asema hakee päivitykset sen ollessa internet yhteydessä. Tärkeää on kuitenkin muistaa, että WTG -työasemat eivät kykene päivittämään Windows -käyttöjärjestelmä versiota. Työasema tulee uudelleen varustaa päivitetyllä näköistiedostolla käyttöjärjestelmän päivittämistä varten. Onkin siis tärkeää päivittää näköistiedosto riittävin väliajoin, ja uudelleen varustaa työasemat päivitetyllä näköistiedostolla mahdollisten käyttöjärjestelmä tietoturva-aukkojen varalta.

Työasemapäivitysprosessia on mahdollista jatkokehittää jälkeenpäin, mikäli laitteesta haluttaisiin myöhemmin IT-hallinnon ylläpitämä. Työasema liitettäisiin organisaation toimialueeseen päivityksen ajaksi, jolloin sisältöpäivitykset voidaan tuottaa kootusti SCCM -hallinnointi palvelimella. WTG -työasemat voidaan määritellä SCCM -hallinnointiohjelmalla omaksi työryhmäksi. Työryhmän päivityksiä voidaan rajoittaa, tai päivittää kootusti määritetyin aikavälein.

5 WINDOWS TO GO OMINAISUUDEN SUOJAUS

5.1 Bitlocker To Go

Kannettavat USB-muistit ovat todella suuressa käytössä perinteisessä tiedon säilytyksessä ja kasvavassa määrin myös työasemina, vrt. Windows To Go ja USB3.0 SSD asemat. Potentiaali laitteen katoamiselle tai varkaudelle on kuitenkin hyvin suuri laitteen ollessa vain tulitikkuaskin kokoinen. Koska USB-muisteihin ei ole mahdollista sijoittaa TPM-sirua kehitti Microsoft, Windows 7 versiosta eteenpäin tiedostonsalaus menetelmän nimeltään Bitlocker To Go (BTG). Toisin kuin USB-asemissa yleisesti käytettävä Encrypting File System (EFS), joka on tiedosto tasoinen tiedostonsalaus, Bitlocker To Go salaa koko siirrettävän aseman. Tiedostonsalaus perustuu 128- tai 256-bittiseen AES tiedostonsalaus algoritmiin, joka on standardoitu lohkosalausmenetelmä. BTG on yhteensopiva NTFS ja kaikkien FAT (FAT32, exFAT, jne.) tiedostojärjestelmien kanssa.
(SystemExperts 2011.)

Kaikessa yksinkertaisuudessaan Bitlocker To Go mahdollistaa USB-muistin tiedostonsalauksen ja rajoittaa sisäänpääsyn salasanalla. Yhdistäessä salatun USB-muistin työasemaan, kysytään sinulta salasanaa, jonka jälkeen saat luku- ja kirjoitusoikeudet asemalle. BTG ei kuitenkaan ole täysin yhteensopiva Windows 7 edeltävien käyttöjärjestelmien kanssa. Liittäessäsi BTG suojatun USB-muistin Windows XP -käyttöjärjestelmään, salasanan syötettyäsi on sinulla vain lukuoikeus asemalle. Tämä ongelma on kuitenkin mahdollista kiertää, mikäli USB-muistin BTG on yhteydessä organisaation toimialueeseen, jossa käytetään Active Directorya. Täältä löytyy asetus, jolla annetaan oikeudet muokata Bitlockerilla-suojattua irrotettavaa asemaa aikaisemmissa Windows versioissa. (Columbia College Information Technology, n.d.)

Bitlocker To Go voidaankin siis määritellä organisaation tarpeiden mukaisiksi Active Directoryn -policyja muuttamalla. Täällä organisaation Group Policy -ylläpitäjä voi muun muassa määritellä BTG pakon kiinnitettäville USB-muisteille, salasana määritykset, lisä tietoturvat kuten älykorttien käytön BTG:n lisäksi ja palautussalasanan tallennus sijainnin.

5.2 **Windows Hardening**

Työasemat joutuvat usein tietoturvahyökkäyksille alttiiksi. Yleisimpiä työaseman saastuttajia ovat internetsivustot, kiinnitettävät mediat, sekä sähköpostiliitteet ja -upotteet. Työasemien ”kovettaminen” onkin varteenotettava lisävaihe tietoturvan parantamiseksi. Työasemien ”kovettamisella” tarkoitetaan työaseman tietoturvan parantamista esimerkiksi karsimalla toimintoja, sekä hallitsemalla tiedoston muutosoikeuksia.

Tärkein työaseman tietoturvalle on ohjelmaversioiden ja käyttöjärjestelmän pitäminen ajan tasalla päivitysten suhteen. Ohjelman version ollessa vanhentunut on hyvin suuri todennäköisyys, että ohjelmalle on löydetty takaportti tai haavoittuvuus. Ohjelmien säännöllinen päivitys on erityisen tärkeää esimerkiksi Microsoft Office ohjelmissa, johon usein ladataan kolmannen osapuolen tiedostoja. (Australian Government 2017.)

Mahdollisia ”kovettamis” kohteita työasemalle löytyy satoja, joita kaikkia ei tässä käydä läpi. Muutama tekniikka mainittakoon, kuten ylläpidon luomat Group Policy -säännöt, ylläpitäjä oikeudet ”root” kansioihin, ylimääräisten ohjelmien ja työkalujen estäminen, salasana käytäntöjen monimutkaisuus, sekä tietoturvaohjelmien käyttö. (Australian Government 2017.)

Käyttäjä voi itse vaikuttaa tietoturvan vaarantumiseen omaksumalla oikeita työtapoja. On syytä käyttää harkintaa, millä sivustoilla käy sekä mitä työasemalleen lataa. Suositeltavaa on myös kiinnitettävien USB-muistien tarkistus tietoturvaohjelmalla ennen sen avaamista. Samaa salasanaa ei tule käyttää useammalla sivustolla tai ohjelmalla ja niiden tulee olla riittävän pitkiä. Tärkein tietoturva työasemalle on loppujen lopuksi käyttäjä itse.

6 YHTEENVETO

Opinnäytetyössäni käsittelin Windows To Go -työaseman ominaisuuksia, sekä käyttöönottoa eri menetelmillä vaihe vaiheelta. Opinnäytetyön aihe oli minulle hyvin mieleinen, sillä sain työskennellä työharjoittelujaksoni aikana jo kyseisen ominaisuuden parissa. Ominaisuuden kehitystyö keskeytyi harjoittelujaksoni aikana, joten oli mukavaa palata takaisin sen pariin. Minulla oli aikaisemmin hyvin vähän kokemusta järjestelmänhallinnoinnista ja Windows asennuspakettien hallinnoinnista ei lainkaan. Opinnäytetyön ja kuluneen työharjoitteluni myötä olen saanut tilaisuuden opiskella ja perehtyä muun muassa SCCM -järjestelmänhallintaohjelman käyttöön teoriassa sekä käytännössä. SCCM on hyvin laajalti käytössä yrityksissä ja organisaatioissa sekä järjestelmien automatisointi on kaiken aikaa yleistymässä, joten uskonkin näiden kokemusten parantavan myös työllisyysnäkymääni. Järjestelmänhallinnoinnissa hienointa on jatkuva kehittämisen ja parantamisen mahdollisuus.

Käyttöönoton ja virtuaalipalvelimen toteuttaminen onnistuivat hyvin, koska olin luonut virtuaaliympäristöjä ja Windows -käyttöjärjestelmäpaketteja jo aikaisemmin työharjoittelussa. WTG-työasemien käyttöönoton pilotointi onnistui ja asennuspaketit olivat toimivia. Ajurit asentuivat koneille onnistuneesti ja BTG-asennusmedia tallentui asennuspakettiin.

Ongelmia työaseman käyttöönotossa esiintyi muutamia virtuaaliympäristön käytöstä johtuen. Asennuspaketteihin sisällytettyjen ohjelmien asentumista ei ollut mahdollista testata, koska ne haetaan vasta asennuksen aikana SCCM jakelupisteeltä. SCCM -palvelin sijaitsi virtuaaliympäristössä ja kiinnitettävää WTG USB-asemaa ei ollut mahdollista kiinnittää virtuaaliympäristöön. Käyttöjärjestelmän automatisoitua aktivointia ei myöskään ollut mahdollista testata pilotoinnissa käytetystä Evaluation käyttöjärjestelmä versiosta johtuen. Jouduin myös luomaan virtuaaliympäristön ja asennusmediat toiseen otteeseen kovalevyn rikkoontumisesta johtuen.

Ominaisuutta on mahdollista jatkokehittää lähes rajattomasti. Asennuspakettiin on helppo lisätä uusia ohjelmia tai ominaisuuksia. Ominaisuuden käyttöönoton kehityskulusta riippuen on mahdollista harkita myös toimialueeseen liittämistä, jolloin päivitykset ja hallinnointi voidaan keskittää ylläpidolle. Näin voitaisiin varmistaa ominaisuuden pysyminen ajan tasalla sekä tietoturva.

Tavoitteenani oli esitellä toimeksiantajalleni korvaava ratkaisu kannettavalle tietokoneelle, sekä dokumentoida laitteen käyttöönotto. Windows To Go -ominaisuus tulisi käyttöön puolustusvoimien henkilökunnalle, muun muassa ulkomaankomennuksille. Palautteen perusteella opinnäytetyön sisältö vastasi toimeksiantajan toiveita ja tarpeita. Lopputulos oli tavoitteeni mukainen, vaikka joitain aiheita jouduin sivuuttamaankin, jottei työ olisi levinnyt liikaa.

Opinnäytetyön aikana opin aikataulutuksen ja suunnittelun tärkeyden projektia tehdessä. Olin aliarvioinut projektiin kuluvan ajan, ja joissain aiheissa kului suunniteltua kauemmin aikaa. Työ vaikutti aluksi huomattavan suurelta, mutta kirjoittamisen aloittamisen jälkeen huomasin työn etenevän hyvin. Työn rungon suunnittelu aivan ensimmäiseksi auttoi minua havainnoimaan projektin kokonaiskuvaa. Joustava, mutta samalla päämäärätietoinen työskentely auttoivat minua edistymään työssäni ja vähentämään työstä johtunutta stressiä.

LÄHTEET

4sysops. (15. Marraskuu 2017). Always on VPN - DirectAccess+ for Windows 10. Haettu 4. 3 2018 osoitteesta https://4sysops.com/archives/always-on-vpn-directaccess-for-windows-10/

Australian Government. (joulukuu 2017) Hardening Microsoft Windows 10, version 1709 Workstations. Haettu 11. 4 2018 osoitteesta https://www.asd.gov.au/publications/protect/Hardening_Win10.pdf

Ballew, J. (2016). Windows to Go, A Guide for Users and IT Professionals. New York: Apress Media LLC.

Columbia College Information Technology. (n.d). Bitlocker to go: Removable Storage Encryption. Haettu 10. 4 2018 osoitteesta https://ccit.college.columbia.edu/knowledge-base/article/bitlocker-go-removable-storage-encryption

Microsoft Licensing. (2018). Frequently asked questions about Volume License keys. Haettu 22.2.2018 osoitteesta https://www.microsoft.com/en-us/licensing/existing-customer/faq-product-activation.aspx

Microsoft Technet, the scripting guys. (28. syyskuu 2015). USE Powershell to create Windows to go keys – part 1-5. Haettu 25. 2 2018 osoitteesta https://blogs.technet.microsoft.com/heyscriptingguy/2015/09/28/use-powershell-to-create-windows-to-go-keys-part-1/

Microsoft. (1. toukokuu 2013). Announcing Windows to Go Certified Drive Partners. Haettu 22.2.2018 osoitteesta https://blogs.windows.com/business/2013/02/01/announcing-windows-to-go-certified-drive-partners/

Microsoft. (19. huhtikuu 2017) Deploy Windows to Go in your organization. Haettu 13.2.2018 osoitteesta https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-to-go

Microsoft. (19. huhtikuu 2017) Deployment considerations for Windows to go. Haettu 20. 3 2018 osoitteesta https://docs.microsoft.com/en-us/windows/deployment/planning/deployment-considerations-for-windows-to-go

Microsoft. (19. huhtikuu 2017). Best practice recommendations for Windows to Go. Haettu 7.2.2018 osoitteesta https://docs.microsoft.com/en-us/windows/deployment/planning/best-practice-recommendations-for-windows-to-go

Microsoft. (19. huhtikuu 2017). Windows to Go: feature overview. Haettu 19.1.2018 osoitteesta https://docs.microsoft.com/en-us/windows/deployment/planning/windows-to-go-overview

Microsoft. (2018). Windows Imaging File Format (WIM). Haettu 2.2.2018 osoitteesta https://msdn.microsoft.com/en-us/library/windows/desktop/dd861280.aspx

Microsoft. (6. lokakuu 2016). Deploy Windows to Go with System Center Configuration Manager. Haettu 18.3.2018 osoitteesta https://docs.microsoft.com/en-us/sccm/osd/deploy-use/deploy-windows-to-go

Microsoft. (9. helmikuu 2018) Task sequence built-in variables in system center configuration manager. Haettu 9. 4 2018 osoitteesta https://docs.microsoft.com/en-us/sccm/osd/understand/task-sequence-built-in-variables

Richard M. Hicks Consulting, Inc. (8. toukokuu 2012). Microsoft Windows DirectAccess Overview. Haettu 4.2.2018 osoitteesta https://directaccess.richardhicks.com/2012/05/08/microsoft-windows-directaccess-overview/

SystemExperts. (2011). How to Use Bitlocker To Go in Windows 7: A Primer. Haettu 9. 3 2018 osoitteesta https://systemexperts.com/pdf/SystemExperts-What_is_BitLocker_Pt1-2.pdf

Trusted Computing Group. (1. huhtikuu 2008). Trusted Platform Module (TPM) Summary. Haettu 15.2.2018 osoitteesta https://trustedcomputinggroup.org/trusted-platform-module-tpm-summary/

University of Nebraska-Lincoln. (2018). Microsoft SCCM FAQ. Haettu 18.3.2018 osoitteesta https://its.unl.edu/desktop/microsoft-sccm-faq